SPECIAL DOMAINS OF RATIONALITY

BY

JESSE ERNEST WILKINS

THESIS

FOR THE

DEGREE OF BACHELOR OF ARTS

IN

MATHEMATICS

COLLEGE OF LIBERAL ARTS AND SCIENCES

UNIVERSITY OF ILLINOIS

1918

UNIVERSITY OF ILLINOIS

May 21, 1918

THIS IS TO CERTIFY THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Jesse Ernest Wilkins

ENTITLED SPECIAL DOMAINS OF RATIONALITY

IS APPROVED BY ME AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF Bachelor of Arts in Mathematics

L. A. Miller

Instructor in Charge

APPROVED: E. J. Townsend

HEAD OF DEPARTMENT OF Mathematics

TABLE OF CONTENTS

Chapter IV

The Domain $K(\sqrt{-5})$

Chapter V

Finite Domains with respect to Certain Prime and Double Moduli

SPECIAL DOMAINS OF RATIONALITY

Introduction

The expression "Domain of Rationality"* was introduced into the science of mathematics by L. Kronecker at least as early as 1881, and has practically the same meaning as "Körper" introduced by Dedekind a few years earlier. It represents a system of different numbers permitting without reserve the fundamental operations: addition, subtraction, multiplication and division. The result of all these operations, except division by 0, made upon the numbers of the system give also a number of the system.

All rational numbers, integers and rational fractions taken both positively and negatively, constitute such a domain, for this system of magnitudes is complete in itself in the sense that any of the four operations involving any of these numbers never yields as a result a number which does not belong to the set.

The integers by themselves do not constitute a domain, for the quotient of two integers may be fractional.

Another example of a domain of numbers is the one embracing all real numbers, whether rational or irrational. Still another is the domain consisting of all numbers, $a + bi$, where a and b are rational or irrational and $i = \sqrt{-1}$.

The domain of rational numbers is a divisor of all domains, that is, it is contained in all domains, for each domain contains at least one number, n, different from 0; hence it contains $n \div n$ or 1. But if unity belongs to the domain, then it embraces all

---

* Journal für die Mathematik: Vol. 92, p. 1.

numbers obtained by addition and subtraction of units, that is, all positive and negative integers; from the latter we can derive all rational fractions. Hence the rational numbers occur in every domain. The domain of rational numbers is usually indicated by R.

Generation of a Domain.

If α be any algebraic number, the system consisting of all numbers which can be formed by repeated operations upon α of the four fundamental operations, that is, the system consisting of all rational functions of α with rational coefficients, will be a domain. For the sum, difference, product and quotient of any two rational functions of α are rational functions of α and hence numbers of the system. We say that α generates this domain. We say also that α defines this domain and represent the latter by $K(\alpha)$. The rational domain can be generated by any rational number, a; for a divided by a gives 1, and from 1 by repeated additions and subtractions of 1, we can obtain all rational integers, and from them by division all rational fractions. As the number defining the rational domain we generally take 1, thus denoting the domain by K(1). As has been stated however the rational domain is usually denoted by the letter R. The domain of complex numbers, $a+bi$, can be generated by i; for i divided by i gives 1, and from 1 we can generate the rational domain and then by multiplying i by all rational numbers in turn and adding to each of these products each rational number in turn, we obtain all numbers of the form $a+bi$, where a and b take all rational values. This domain is therefore denoted by K(i). It is well to observe that although i is the number which most conveniently defines K(i) and is indeed the one usually selected, it is not the only number that will serve this

purpose. On the contrary, this domain can be generated by any number of the form $c+di$ where c and d are rational numbers, and $d \neq 0$; that is, $K(i)$ and $K(c+di)$ are identical; for since $K(c+di)$ contains R it contains c and d and hence $\frac{c+di-c}{d} = i$. Therefore $K(c+di)$ contains all numbers of $K(i)$. Moreover since $K(i)$ contains $c+di$, it contains all numbers of $K(c+di)$. Hence $K(i)$ is identical with $K(c+di)$.

The plan of the paper will be as follows. The first four chapters will be devoted to a discussion of four special quadratic domains in the following order: $K(i)$, $K(\sqrt{-3})$, $K(\sqrt{2})$, $K(\sqrt{-5})$. We shall find that the properties of an integer will depend upon the domain in which it is considered to lie. Thus the integer 5 is unfactorable in R and in $K(\sqrt{-3})$ but in $K(i)$ it is the product of two integers, $2+i$ and $2-i$. In the cases of $K(i)$, $K(\sqrt{-3})$ and $K(\sqrt{2})$, we shall see that, with the introduction of a few new conceptions, the integers of these domains obey in their relations to each other laws almost identical with those governing the integers of R. In the case of $K(\sqrt{-5})$ we shall notice an important difference, and at first sight it will seem that the old laws have no analogies in this domain. By the introduction, however, of the conception of the ideal number the difficulties of this particular domain will be overcome. Chapter V will be devoted to the discussion of certain finite domains with respect to certain prime and double moduli.

Chapter I

The Domain K(i)

The number i is defined by the equation

$$X^2+1 = 0$$

which it satisfies. Every number of K(i) is a rational function of i with rational coefficients, and since by means of the relation $i^2 = -1$ the degree of any rational function of i may be reduced so as to be not higher than the first, every number, α, of K(i) has the form

$$\alpha = \frac{a_1+b_1 i}{a_2+b_2 i},$$

where a_1, b_1, a_2, b_2 are rational numbers, or multiplying the numerator and denominator of this fraction by $a_2-b_2 i$, we have

$$\alpha = \frac{a_1 a_2+b_1 b_2}{a_2^2+b_2^2} + \frac{a_2 b_1-a_1 b_2}{a_2^2+b_2^2} i;$$

that is, every number, α, of K(i) has the form

$\alpha = a+bi$, where a and b are rational numbers.

The process of addition in this domain always gives a number in the domain; moreover this operation is unique. It is very obvious that if we add two numbers in this domain we will obtain as a result another number of the domain; that this operation is also unique is seen from the following:

If $\alpha+\beta = \gamma$

and also $\alpha+\beta_1 = \gamma$, where $\beta_1 \neq \beta$,

it would follow that $\beta-\beta_1 = 0$. This is impossible unless $\beta = \beta_1$; but this is contrary to our hypothesis that $\beta_1 \neq \beta$. We see then that the operation is unique.

Similarly the uniqueness of the process of subtraction may be established.

The process of multiplication in this domain always gives a number in the domain and we see that this operation is also unique from the following:

If α and β are two numbers of the domain and $\alpha\beta = \gamma$, and also $\alpha\beta_1 = \gamma$, where β_1 is another number of the domain different from β, it would follow that $\alpha(\beta - \beta_1) = 0$. This is impossible unless $\alpha = 0$ or $\beta - \beta_1 = 0$. $\alpha \neq 0$, therefore $\beta = \beta_1$. But this is contrary to our hypothesis that they were different from each other.

The process of division (division by 0 excluded) in this domain always gives a number in the domain; moreover this operation is in general unique.

If α and γ are any two numbers of the domain it is necessary to show that there is a number, β, in the domain such that

$$\alpha = \beta\gamma;$$

if we assign to β all the values of the different numbers of the domain and multiply γ by these different values of β (since multiplication is possible and unique in the domain) we will obtain all of the numbers of the domain once and only once. Since by hypothesis α is a number of the domain, it is obtained when γ is multiplied by some one of the values assigned to β. We see therefore that $\alpha/\beta = \gamma$ ($\beta = 0$ excluded) is always possible in the domain.

If $\alpha/\beta = \gamma$,

and also $\alpha/\beta_1 = \gamma$, where $\beta_1 \neq \beta$,

it follows that $\gamma(\beta - \beta_1) = 0$. This equation can not be true unless $\gamma = 0$ or $\beta - \beta_1 = 0$; excluding the trivial case $\alpha = 0$. Therefore $\beta - \beta_1 = 0$ or $\beta = \beta_1$. We see then that this operation in general

is unique.

Algebraic Integers of K(i)

Before attempting to determine the algebraic integers of K(i) it is necessary to define what we mean by a primitive number, an algebraic number and an algebraic integer.

A primitive number is defined as any number which satisfies an irreducible rational equation of the same degree as that of the domain.

A number, α, is called an algebraic number when it satisfies an equation of the form

$$X^n + a_1 X^{n-1} + \ldots\ldots\ldots a_{n-1} X + a_n = 0 \qquad (1)$$

where $a_1, a_2, \ldots\ldots, a_n$ are rational numbers.

An algebraic integer is defined as any algebraic number which satisfies an equation of the form (1) whose coefficients, $a_1, a_2, \ldots\ldots\ldots, a_n$, are rational integers.

It might be interesting to note that not all numbers are algebraic numbers; for instance, π and e(base of natural logarithms) which are transcendental numbers. The proof of the existence of such numbers will not be attempted in this paper.

With these definitions in mind we are able to determine when a primitive number, α, is an algebraic integer by observing that the necessary and sufficient condition that α shall be an algebraic integer is that the coefficients of the single equation of the lowest degree,

$$X^2 + PX + Q = 0,$$

satisfied by α shall be integers.

But $$-P = \alpha + \alpha', \text{ and } Q = \alpha\alpha'$$

and hence the necessary and sufficient conditions that α shall be

an algebraic integer are that $\alpha + \alpha'$ and $\alpha\alpha'$ shall be rational integers.

If we write α in the form $a+bi$, where $a = a_1/c_1$, and $b = b_1/c_1$, a_1, b_1, c_1 being rational integers with no common factor, although any two of them may have a common factor, these conditions become

$$\frac{a_1+b_1 i}{c_1} + \frac{a_1-b_1 i}{c_1} = \frac{2a_1}{c_1} = \text{a rational integer}, \qquad (1)$$

$$\left(\frac{a_1+b_1 i}{c_1}\right)\left(\frac{a_1-b_1 i}{c_1}\right) = \frac{a_1^2+b_1^2}{c_1^2} = \text{a rational integer}, \qquad (2)$$

One at least of the three following cases must occur:

A. $c_1 \neq 2$ or 1; B. $c_1 = 2$; C. $c_1 = 1$.

The impossibility of A and B can be easily demonstrated.

A. If $c_1 \neq 2$ or 1, then by virtue of (1) a_1 and c_1 would have a common factor that by virtue of (2) would be contained in b_1 also. But this is contrary to our hypothesis that a_1, b_1, c_1 have no common factor. Hence A is impossible.

B. If $c_1 = 2$ then $a_1^2+b_1^2$ would be divisible by 4. We shall show that the necessary and sufficient condition that $a_1^2+b_1^2$ be divisible by 4 is that a_1 and b_1 each be divisible by 2. If either a_1 or b_1 is even then the square of the even one is divisible by 4, but since their sum must also be divisible by 4 the square of the other one must also be divisible by 4 and hence be even. If a_1 and b_1 are both even a_1, b_1 and c_1 have a common factor.

If a_1 and b_1 are both odd we may write them in the form

$$a_1 = 2k_1 \pm 1,$$
$$b_1 = 2k_2 \pm 1.$$

Then $$a_1^2+b_1^2 = 4(k_1^2+k_2^2) \pm 4(k_1+k_2) + 2.$$

We see that this expression when divided by 4 does not give a rational integer. Therefore B is impossible since $a_1^2+b_1^2$ is divisible by 4 only when a_1, b_1 and c_1 have a common factor.

Hence $c_1 = 1$; that is a and b are rational integers.

We see then that all algebraic integers of K(i) have the form $a+bi$, where a and b are rational integers and all numbers of this form are integers of K(i). If $b = 0$, we obtain the rational integers. In K(i), as in R, the sum, difference and product of any two integers are integers.

Prime Numbers of K(i)

A unit of K(i) is an integer which is a divisor of every integer of K(i). The units of K(i) are 1, -1, i and -i.

In the rational domain, two integers, r and -r, that differ only by a unit factor are said to be associated, so in K(i) the four integers, α, $-\alpha$, $i\alpha$, and $-i\alpha$, obtained by multiplying any integer, α, by the four units in turn, are called the associates of α.

Bearing in mind the above definitions of a unit and associates we shall define a prime number of K(i) as an integer of K(i) that is not a unit and that has no divisors other than its associates and the units.

A composite number of K(i) is defined as an integer of K(i) that has divisors other than its associates and the units.

These definitions are identical with the corresponding ones in the rational domain. To ascertain whether any integer, α, not a unit, is a composite or prime number of K(i), it is only necessary to determine whether or not α can be resolved into two factors neither of which is a unit. We therefore put

$$\alpha = (a+bi)(c+di)$$

and determine for what sets of integral values of a, b, c and d

this equation is satisfied. If any one of these sets of values be such that neither $a+bi$ nor $c+di$ is a unit, α is a composite number; but, if for every set of values one of these factors be a unit, α is a prime.

It is hoped that the introduction of the two following examples will make the conception of prime and composite numbers of K(i) clearer.

Ex. 1. To determine whether 7 is a prime or composite number of K(i).

Put $$7 = (a+bi)(c+di);$$

then $$n(7)^* = 49 = (a^2+b^2)(c^2+d^2),$$

whence we have either

$$\begin{matrix} a^2+b^2 = 7 \\ c^2+d^2 = 7 \end{matrix} \quad (1) \quad \text{or} \quad \begin{matrix} a^2+b^2 = 1 \\ c^2+d^2 = 49 \end{matrix} \quad (2)$$

Remembering that a, b, c and d must be rational integers, we see that (1) is impossible, while from (2) it follows that $a+bi$ is a unit. Therefore 7 is a prime number of K(i).

Ex. 2. To determine whether $7+6i$ is a prime or composite number of K(i).

Put $$7+6i = (a+bi)(c+di);$$

then $$n(7+6i) = 85 = (a^2+b^2)(c^2+d^2),$$

whence we have either

$$\begin{matrix} a^2+b^2 = 5 \\ c^2+d^2 = 17 \end{matrix} \quad (1) \quad \text{or} \quad \begin{matrix} a^2+b^2 = 1 \\ c^2+d^2 = 85 \end{matrix} \quad (2)$$

From (2) it would follow that $a+bi$ is a unit, but (1) gives

---

* The norm of a number, α, is defined as the product of the number, α, by its conjugate and is denoted by $n(\alpha)$. For example:

$$n(a+bi) = (a+bi)(a-bi) = a^2+b^2,$$
$$n(4+i) = (4+i)(4-i) = 17,$$
$$n(7) = 7 \cdot 7 = 49.$$

The norms of all numbers of K(i) are positive rational numbers.

$$a = \pm 2, \quad b = \pm 1, \quad c = \pm 4, \quad d = \pm 1, \qquad \text{or} \qquad a = \pm 1, \quad b = \pm 2, \quad c = \pm 1, \quad d = \pm 4,$$

whence $a+bi = \pm(2+i)$ or $\pm(1-2i)$ (3)
or $a+bi = \pm(2-i)$ or $\pm(1+2i)$ (4)
and $c+di = \pm(4+i)$ or $\pm(1-4i)$ (5)
or $c+di = \pm(4-i)$ or $\pm(1+4i)$ (6)

the four integers after each sign of equality being associated.

This process gives us not only the divisors of $7+6i$ and its associates, but also the divisors of every other integer whose norm is 85; that is, of $7-6i$, $9+2i$, $9-2i$, and their associates. Each one of the eight values of $a+bi$ multiplied by any one of the eight values of $c+di$ gives an integer whose norm is 85.

Selecting by trial the divisors of $7+6i$, we see that any integer from (3) multiplied by a suitable one from (5), gives $7+6i$.

Thus $$7+6i = (2+i)(4+i) \qquad (7).$$

Hence $7+6i$ is a composite number of K(i).

We have also
$$\begin{aligned} 7+6i &= (1-2i)(-1+4i), \\ &= (-1+2i)(1-4i), \\ &= (-2-i)(-4-i), \end{aligned}$$

but these factorizations are looked upon as in no way different from (7) since the corresponding factors are associated. Hence $7+6i$ can be factored in only one way into two prime factors*, neither of which is a unit. If now we attempt to factor $2+i$ and $4+i$, we find that they are prime numbers, and hence we say that $7+6i$ has been resolved into its prime factors.

Classification of the Prime Numbers of K(i)

Remembering that every prime, π, of K(i) divides an infinite number of positive rational integers, for example, $n(\pi)$ and its

---

* A general proof of the unique factorization theorem for K(i) is given on pp. 14-19 of this paper.

multiples, we are able to classify the rational primes which are considered as integers of K(i). Among these positive rational integers there will be a smallest one, p, and p will be a rational prime number, for if p be not a prime, that is, if $p = p_1 p_2$, π would divide either p_1 or p_2, and hence p would not be the smallest rational integer that π divides. In order therefore, to determine all rational primes of K(i) it is only necessary to examine all rational primes considered as integers of K(i).

It is also evident that no prime of K(i) can divide two different rational primes, for then it would divide their rational greatest common divisor, 1, hence be a unit. We see therefore that every prime of K(i) occurs once and but once among the divisors of the rational primes considered as integers of K(i).

Denoting then by p the smallest rational prime that π divides we have

$$p = \pi\alpha$$

and hence

$$p^2 = n(\pi)\, n(\alpha) \qquad (1)$$

We then have two cases:

A. $n(\pi) = p$, $n(\alpha) = p$ B. $n(\pi) = p^2$, $n(\alpha) = 1$

The case $n(\pi) = 1$ is excluded because the only numbers of K(i) whose norms are unity are the units.

A. From $n(\pi) = \pi\pi' = p$ and (1) it follows that $\alpha = \pi'$. If $\pi = a + bi$, we have then

$$p = n(a + bi) = a^2 + b^2.$$

If we assume $p \neq 2$, then a or b must be odd and the other even. Suppose a is even, then b must be odd; a and b may then be written

$$a = 2m$$
$$b = 2m_1 \pm 1.$$

Then $a^2 + b^2 = 4(m^2 + m_1^2 \pm m_1) + 1$, or $a^2 + b^2$ is of the form $4h + 1$, where $h = m^2 + m_1^2 \pm m_1$.

We see then that when a positive rational prime other than 2 is the product of two conjugate primes of K(i), it has the form $4h+1$.

The above fact is also expressed in the following manner: If a positive rational prime, p, other than 2 is the product of two conjugate primes of K(i), then p is congruent to 1, modulus 4, and is usually written

$$p \equiv 1, \text{ mod } 4.$$

The term congruence is defined in the following manner: if we have two integers, a and b, and if the difference of a and b is divisible by another integer c, a and b are said to be congruent to each other with respect to the modulus c. This relation is expressed thus

$$a \equiv b, \text{ mod } c.$$

When $p = 2$, we have

$$2 = (1+i)(1-i),$$

and hence

$$2 = i(1-i)^2;$$

it follows then that 2 is associated with, and hence divisible by the square of a prime of K(i).

B. Since $n(\alpha) = 1$, α is a unit and hence p is associated with the prime π; that is , p is a prime in K(i). We see then that a rational prime p is either a prime of K(i) or is the product of two conjugate primes of K(i).

Therefore when p is a rational prime of the form $4h-1$ it is always a prime in K(i), for we have just seen above that p is factorable into two conjugate primes of K(i) only when it is 2 or of the form $4h+1$.

Using the notation of congruence we say that a rational prime p when congruent to -1, modulus 4, is always a prime in K(i).

We have shown above that every rational prime which is the

product of two conjugate primes of K(i) is of the form 4h + 1; it is now necessary to show that every rational prime of the form 4h + 1 can be represented as the product of two conjugate primes of K(i).

Since p is of the form 4h + 1, it follows that

$$p \equiv 1, \text{ mod } 4$$

Our first task is to show that from this fact it follows that the congruence

$$X^2 \equiv -1, \text{ mod } p, \text{ has roots.}$$

Euler has proved that the necessary and sufficient condition that a is a quadratic residue of p, that is, that the congruence

$$X^2 \equiv a, \text{ mod } p,$$

shall have roots is

$$a^{\frac{p-1}{2}} \equiv 1, \text{ mod } p.*$$

In our particular problem it is necessary to show that -1 is a quadratic residue of p when p is of the form 4h + 1. Accepting Euler's criterion we raise -1 to the $\frac{p-1}{2}$ power and if it is congruent to 1, mod p, it is a quadratic residue of p.

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4h+1-1}{2}} = (-1)^{2h} = 1,$$

therefore $$(-1)^{\frac{p-1}{2}} \equiv 1, \text{ mod } p.$$

We see therefore that the congruence

$$X^2 \equiv -1, \text{ mod } p, \text{ has roots.}$$

Let a be a root. Then

$$a^2 \equiv -1, \text{ mod } p,$$

and hence $$(a+i)(a-i) \equiv 0, \text{ mod } p.$$

Since a + i and a − i are integers of K(i), the integer p, if a prime of K(i), must divide either a + i or a − i. This is however

---

* L. W. Reid: The Elements of the Theory of Algebraic Numbers, p. 115.

impossible, for from

$$a \pm i = p(c + di),$$

where $c + di$ is an integer of K(i), it would follow that $pd = \pm 1$, which can not hold since p and d are both rational integers and $p > 1$. Hence p is not a prime in K(i), and since the only way in which a rational prime can be factored in K(i) is into two conjugate prime factors, p is factorable in this manner.

From the above results, we see that the primes of K(i) may be classified in the following manner, according to the rational primes of which they are factors.

(1) All rational primes of the form $4h + 1$ are factorable in K(i) into two conjugate primes.

(2) All positive rational primes of the form $4h - 1$ are primes in K(i).

(3) The number 2 is associated with the square of a prime of the first degree.

The Unique Factorization Theorem for K(i)

According to the definition, every composite number of K(i) can be resolved into the product of two factors, neither of which is a unit. One or both of these factors may be composite, and hence in turn resolvable into two factors, neither of which is a unit, and we can continue this process until we reach factors which are primes. It is evident that when one or both of the factors are composite, the resolution is not unique. We shall show that, when the resolution is continued until the factors are primes, it will be unique, considering associated factors as the same, and that such a resolution is possible.

To prove this theorem for K(i), that is, that every integer

of K(i) can be represented in one and only one way as a product of prime numbers, we require the following theorems:

Theorem 1. *If α be any integer of K(i), and β any integer of K(i) different from 0, there exists an integer γ of K(i) such that*

$$n(\alpha-\gamma\beta) < n(\beta).$$

Let $\alpha/\beta = a+bi$, where $a = r+r_1$, $b = s+s_1$, r and s being the rational integers nearest to a and b respectively, and hence

$$|r_1| \leq 1/2, \quad |s_1| \leq 1/2$$

We are able to show that γ, $= r+si$, will fulfil the required conditions of the theorem.

$$\alpha/\beta - \gamma = r+r_1+si+s_1i-r-si = r_1+s_1i.$$

Since $\alpha/\beta - \gamma = r_1+s_1i$

$$n(\alpha/\beta-\gamma) = r_1^2+s_1^2 \leq 1/2;$$

whence $n(\alpha/\beta-\gamma) < 1$; or, multiplying by $n(\beta)$,

$$n(\alpha-\gamma\beta) < n(\beta).$$

The following example will illustrate the theorem.

If $\alpha = 4+i$, and $\beta = 3+2i$

$$\frac{\alpha}{\beta} = \frac{4+i}{3+2i} = \frac{14}{13} - \frac{5}{13}\,i$$

and $$\gamma = 1-i.$$

Therefore $\alpha-\gamma\beta = 4+i-(1-i)(3+2i) = -1+2i.$

$$n(-1+2i) = 5$$
$$n(3+2i) = 13$$

Hence $n(-1+2i) < n(3+2i)$.

Theorem 2. *If α and β be any two integers of K(i) prime to each other, there exist two integers μ and ν of K(i) such that*

$$\alpha\mu+\beta\nu = 1.$$

We see readily that if either α or β be a unit, the existence of the required integers μ, ν, is evident. Our task is to show that, if neither α nor β be a unit the determination of μ and ν

can be made to depend upon the determination of a corresponding pair of integers u_1, v_1, for a pair of integers α_1, β_1, prime to each other and such that the norm of one of them is less than both $n(\alpha)$ and $n(\beta)$.

If we assume that $n(\beta) \leq n(\alpha)$ the generality of the proof will not be limited.

In Theorem 1 we proved the existence of an integer γ such that

$$n(\alpha - \gamma\beta) < n(\beta).$$

β and $\alpha - \gamma\beta$ are then a pair of integers, α_1, β_1, prime to each other and $n(\alpha - \gamma\beta)$ is less than both $n(\alpha)$ and $n(\beta)$. If now two integers, u_1, v_1, exist such that

$$\alpha_1 u_1 + \beta_1 v_1 = 1$$

that is,
$$\beta u_1 + (\alpha - \gamma\beta) v_1 = 1,$$

we have
$$\alpha v_1 + \beta(u_1 - \gamma v_1) = 1,$$

and hence
$$u = v, \qquad v = u_1 - \gamma v_1$$

The determination of u_1, v_1, for α_1, β_1, may if neither α_1 nor β_1 be a unit, be made to depend similarly upon that of u_2, v_2, for a pair of integers α_2, β_2 prime to each other and such that the norm of one of them is less than both $n(\alpha_1)$ and $n(\beta_1)$.

If we continue this process, we are able always to make the determination of u and v depend eventually upon that of u_n, v_n for a pair of integers α_n, β_n, one of which is a unit. Since the existence of u_n, v_n, is evident , the existence of u and v is proved.

Theorem 3. <u>If the product of two integers, α and β of K(i) be divisible by a prime number, λ, at least one of the integers is divisible by λ.</u>

Let $\alpha\beta = \gamma\lambda$, where γ is an integer of K(i), and assume α not to be divisible by λ. Then α and λ are prime to each other and

from Theorem 2 we see that there exist two integers of K(i), μ and ν such that

$$\alpha\mu+\lambda\nu = 1 \qquad (1)$$

multiplying (1) by β, we obtain

$$\beta\alpha\mu+\beta\lambda\nu = \beta,$$

and therefore $\lambda(\gamma\mu+\beta\nu) = \beta$, for $\alpha\beta = \gamma\lambda$

where $\gamma\mu+\beta\nu$ is an integer of K(i). Therefore since β is the product of λ and $\gamma\mu+\beta\nu$, β is divisible by λ.

We are now in a position to state and prove the Unique Factorization Theorem.

Every integer of K(i) can be represented in one and only one way as the product of prime numbers.

Let α be an integer of K(i); if α be not itself a prime number, we have

$$\alpha = \beta\gamma \qquad (2)$$

where β and γ are integers of K(i) neither of which is a unit. From (2) it follows that $n(\alpha) = n(\beta)\, n(\gamma)$; moreover, since $n(\beta) \neq 1$ and $n(\gamma) \neq 1$ we have $n(\beta)$ and $n(\gamma) < n(\alpha)$.

If β be not a prime number, we have as before

$$\beta = \beta_1\gamma_1$$

where β_1 and γ_1 are integers neither of which is a unit, and hence $n(\beta_1)$ and $n(\gamma_1) < n(\beta)$. If β_1 be not a prime number, we proceed in the same manner, and since $n(\beta)$, $n(\beta_1)$, $n(\beta_2)$, ... form a decreasing series of positive rational integers, we will reach after a finite number of such factorizations in the series β, β_1, β_2, ... a prime number λ_1. Thus α has the prime factor λ_1, and we have

$$\alpha = \lambda_1\alpha_1.$$

Proceeding similarly with α_1, in case it is not a prime number, we obtain

$$\alpha_1 = \lambda_2\alpha_2$$

where λ_2 is a prime number, and hence

$$\alpha = \lambda_1 \lambda_2 \alpha_2$$

If we continue this process we will reach in the series $\alpha, \alpha_1, \alpha_2,$ . . . . . a prime number λ_n, since $n(\alpha), n(\alpha_1), n(\alpha_2), \ldots\ldots$ form a decreasing series of positive rational integers. We thus have

$$\alpha = \lambda_1 \lambda_2 \lambda_3 \cdots\cdots \lambda_n$$

where the λ's are all prime numbers; that is α can be represented as a product of a finite number of factors all of which are prime numbers.

The Unique Factorization Theorem for K(i) will be completely proved if we can now establish the fact that the above representation is unique.

Suppose that $$\alpha = \rho_1 \rho_2 \rho_3 \cdots\cdots \rho_n$$

is a second representation of α as a product of prime factors. It follows from Theorem 3, from

$$\lambda_1 \lambda_2 \lambda_3 \cdots\cdots \lambda_n = \rho_1 \rho_2 \rho_3 \cdots\cdots \rho_n \qquad (3)$$

that at least one of the ρ's, say ρ_1, is divisible by λ_1, and hence associated with λ_1; that is, $\rho_1 = \epsilon_1 \lambda_1$, where ϵ is a unit. Dividing (3) by λ_1, we have

$$\lambda_2 \lambda_3 \cdots\cdots \lambda_n = \epsilon_1 \rho_2 \rho_3 \cdots\cdots \rho_n$$

From this it follows that at least one of the remaining ρ's, say ρ_2, is divisible by λ_2, and hence associated with it. Thus $\rho_2 = \epsilon_2 \lambda_2$, where ϵ_2 is a unit, and hence

$$\lambda_3 \cdots\cdots \lambda_n = \epsilon_1 \epsilon_2 \rho_3 \cdots\cdots \rho_n$$

If we continue in this manner, we shall see that with each λ there is associated at least one ρ, and, if two or more λ's be associated with one another, at least as many ρ's are associated

with these λ's , and hence with one another.

In precisely the same manner we are able to prove that with each ρ there is associated at least one λ, and, if two or more ρ's be associated with one another, at least as many λ's are associated with these ρ's, and hence with one another.

We see now, considering two associated factors as the same, that the two representations are identical; that is, if in the one representation there occur e factors associated with a certain prime, there will also be in the other representation exactly e factors associated with the same prime. Since these representations are identical we can evidently write every integer, α, of K(i) in the form

$$\alpha = \epsilon \lambda_1^{e_1} \lambda_2^{e_2} \cdots \cdots \lambda_n^{e_n}$$

where $\lambda_1, \lambda_2, \ldots\ldots, \lambda_n$ are the unassociated prime factors of α, and ϵ is a suitable unit; and this representation is unique.

Chapter II

The Domain $K(\sqrt{-3})$

The number $\sqrt{-3}$ is defined by the equation

$$X^2+3 = 0,$$

which it satisfies. It can be shown exactly as in K(i) that all numbers of $K(\sqrt{-3})$ have the form $a+b\sqrt{-3}$, where a and b are rational numbers. Just as in K(i) every number, $\alpha = a+b\sqrt{-3}$, of $K(\sqrt{-3})$ satisfies a rational equation of the second degree, that being the degree of the domain. By using the same method of proof as in K(i) it can be shown that the fundamental operations in this domain always give a number in the domain, and that these operations are in general unique.

Algebraic Integers of $K(\sqrt{-3})$

Since the domain $K(\sqrt{-3})$ is of the second degree, an algebraic integer of $K(\sqrt{-3})$ is defined as an algebraic number which satisfies an equation of the form

$$X^2+PX+Q = 0$$

where P and Q are rational integers.

The necessary and sufficient conditions that any number, $\alpha = a+b\sqrt{-3}$, of $K(\sqrt{-3})$ shall be an integer are therefore

$$-P = \alpha+\alpha' = \text{a rational integer},$$

and

$$Q = \alpha\alpha' = \text{a rational integer}.$$

If α is written in the form

$$\frac{a_1+b_1\sqrt{-3}}{c_1},$$

where $a = a_1/c_1$, and $b = b_1/c_1$, a_1, b_1, c_1, being integers with no common factor, although any two of them may have a common factor, these conditions become

$$\frac{a_1+b_1\sqrt{-3}}{c_1}+\frac{a_1-b_1\sqrt{-3}}{c_1}=\frac{2a_1}{c_1}=\text{a rational integer,} \qquad (1)$$

$$\left(\frac{a_1+b_1\sqrt{-3}}{c_1}\right)\left(\frac{a_1-b_1\sqrt{-3}}{c_1}\right)=\frac{a_1^2+3b_1^2}{c_1^2}=\text{a rational integer,} \qquad (2)$$

One at least of the three following cases must occur:

A. $c_1 \neq 2$ or 1; B. $c_1 = 2$; C. $c_1 = 1$.

A. The impossibility of A is proved as in K(i).

B. If $c_1 = 2$, $2a_1/c_1$ can be an integer, and yet a_1 not contain the factor 2, $a_1^2+3b_1^2$ being divisible by 4 when a_1 and b_1 are both odd. If a and b are both odd we may write them in the form

$$a_1 = 2k_1 \pm 1,$$
$$b_1 = 2k_2 \pm 1.$$

Then $a_1^2+3b_1^2 = 4(k_1^2 \pm k_1) \pm 12(k_2^2 \pm k_2) + 4$; and we see that 4 is a factor of this expression.

Hence $c_1 = 2$, in which case a_1 and b_1 must both be odd; or $c_1 = 1$.

Therefore every integer of $K(\sqrt{-3})$ has the form $1/2(a+b\sqrt{-3})$, where a and b are either both odd or both even, and all numbers of $K(\sqrt{-3})$ of this form are integers.

We shall now show that every integer of $K(\sqrt{-3})$ can be expressed in the form $s+t\rho$, $\rho = 1/2(-1+\sqrt{-3})$.

Let $$\frac{a+b\sqrt{-3}}{2} = s+t\rho,$$

then $$\frac{a+b\sqrt{-3}}{2} = \frac{2s-t}{2}+\frac{t}{2}\sqrt{-3}$$

hence $$a = 2s-t, \quad b = t,$$

or $$s = 1/2(a+t) = 1/2(a+b), \quad t = b.$$

Therefore $$\frac{a+b\sqrt{-3}}{2} = s+t\rho = 1/2(a+b)+b\rho,$$

but $1/2(a+b)$ is a rational integer since a and b are both even or both odd. Hence we see that $\frac{a+b\sqrt{-3}}{2}$ can always be written in the form $s+t\rho$, where s and t are rational integers.

Prime Numbers of $K(\sqrt{-3})$

The definitions of prime and composite numbers of $K(\sqrt{-3})$ are identical with those in K(i). The units of $K(\sqrt{-3})$ are 1, -1, ρ, $-\rho$, ρ^2, $-\rho^2$, obtained by finding values of x and y which satisfy the equation

$$n(\theta) = x^2 - xy + y^2 = (x - 1/2y)^2 + 3/4y^2 = 1,$$

where θ is a unit of the form $x + y\rho$. The associated integers of $K(\sqrt{-3})$ are therefore α, $-\alpha$, $\alpha\rho$, $-\alpha\rho$, $\alpha\rho^2$, $-\alpha\rho^2$, obtained by multiplying any integer, α, by the units in turn.

To determine whether an integer, α, is a prime or composite number in $K(\sqrt{-3})$ we put

$$\alpha = (a + b\rho)(c + d\rho)$$

and determine for what sets of integral values of a, b, c and d this equation is satisfied. If any one of these sets of values be such that neither $a + b\rho$ nor $c + d\rho$ is a unit, α is a composite number; but, if for every set of values one of these factors be a unit, α is a prime number of $K(\sqrt{-3})$.

Ex. 1. To determine whether 5 is a prime or composite number of $K(\sqrt{-3})$.

Put $\quad 5 = (a + b\rho)(c + d\rho);$
then $\quad 25 = (a^2 - ab + b^2)(c^2 - cd + d^2).$

We then have either

$$a^2 - ab + b^2 = 5, \qquad c^2 - cd + d^2 = 5, \tag{1}$$

or

$$a^2 - ab + b^2 = 1, \qquad c^2 - cd + d^2 = 25. \tag{2}$$

From (2) it follows that $a + b\rho$ is a unit. We shall show that (1) is impossible. If

$$a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4 = 5$$

then since a and b are both integers, it follows that

$$|b| \leqq 2 \text{ and similarly } |a| \leqq 2.$$

That the greatest absolute value of b can never be greater than 2

follows from the fact that $(a-b/2)^2$ is always a positive number, and hence the greatest absolute value of $3b^2/4$ can never be greater than 5. We see then that b^2 can never have an integral value greater than 6; or b can never have an integral value greater than 2. That a can not be greater than 2 is proved in a similar manner.

Now if we substitute for b the values 0, ± 1, ± 2, we see that no integral value of a will satisfy (1). Hence (1) is impossible and from (2) it follows that $a+b\rho$ is a unit. Therefore 5 is a prime number in $K(\sqrt{-3})$.

Ex. 2. To determine whether 3 is a prime or composite number of $K(\sqrt{-3})$.

Put $$3=(a+b\rho)(c+d\rho);$$

then $$9=(a^2-ab+b^2)(c^2-cd+d^2),$$

from which we have either

$$a^2-ab+b^2=3, \quad c^2-cd+d^2=3, \tag{3}$$

or

$$a^2-ab+b^2=1, \quad c^2-cd+d^2=9. \tag{4}$$

From (4) it follows that $a+b\rho$ is a unit. If

$$a^2-ab+b^2=(a-b/2)^2+3b^2/4=3,$$

we are able to show by the same method of reasoning employed in Ex. 1. that

$$|b|\leqq 2, \text{ and } |a|\leqq 2.$$

The possible values of b which satisfy (3) are 0, ± 1, ± 2. If we substitute these values of b in (3) we see that

b = 0, gives $a^2=3$, which is impossible,
b = 1, gives $a^2-a+1=3$, and hence a = -1 or 2,
b = -1, gives $a^2+a+1=3$, and hence a = 1 or -2,
b = 2, gives $a^2-2a+4=3$, and hence a = 1,
b = -2, gives $a^2+2a+4=3$, and hence a = -1.

We see then that

$$a+b\rho=\pm(1-\rho), \pm(2+\rho), \text{ or } \pm(1+2\rho).$$

Similarly we can show that

$$c+d\rho=\pm(1-\rho), \pm(2+\rho), \text{ or } \pm(1+2\rho),$$

and we have

$$3 = (1-\rho)(2+\rho) = (-1+\rho)(-2-\rho) = (1+2\rho)(-1-2\rho),$$

the proper combinations of factors being selected by trial. All of these factorizations are, however, considered as identical, since the factors in each resolution are associated with the corresponding factors in the other resolutions. All of these factors can be proved to be primes of $K(\sqrt{-3})$, from which we see that 3 can be resolved into the product of two prime factors in $K(\sqrt{-3})$, and that this resolution is unique. We could have seen directly from the equation defining the domain that

$$3 = -(\sqrt{-3})^2.$$

Therefore since 3 can be resolved into prime factors, neither of which is a unit, 3 is a composite number of $K(\sqrt{-3})$.

Ex. 3. To determine whether $7+2\rho$ is a prime or composite number of $K(\sqrt{-3})$.

Put $$7+2\rho = (a+b\rho)(c+d\rho),$$

then $$39 = (a^2-ab+b^2)(c^2-cd+d^2),$$

from which we have either

$$a^2-ab+b^2 = 3, \quad c^2-cd+d^2 = 13, \qquad (5)$$

or

$$a^2-ab+b^2 = 1, \quad c^2-cd+d^2 = 39, \qquad (6)$$

From (6) it follows that $a+b\rho$ is a unit. As solutions of (5) we have $a = \pm 1,\ b = \pm 1,\ c = \pm 4,\ d = \pm 3.$

Hence $7+2\rho = (1-\rho)(4+3\rho)$, the proper factors being selected by trial. Therefore since $7+2\rho$ can be expressed as the product of two factors, neither of which is a unit, and both of which can be easily shown to be primes of $K(\sqrt{-3})$, it is a composite number of $K(\sqrt{-3})$.

Classification of Prime Numbers of $K(\sqrt{-3})$

If we use the same method of reasoning as in $K(i)$ it becomes

evident that every prime, π, of $K(\sqrt{-3})$ is a divisor of one and only one rational prime. In order therefore to determine what numbers are primes of $K(\sqrt{-3})$, it is only necessary to find the divisors of all rational primes considered as integers of $K(\sqrt{-3})$.

If we let $\pi, = a+b\rho$, be any prime of $K(\sqrt{-3})$ and p the positive rational prime of which π is a divisor, we have

$$p = \pi\alpha,$$

and hence
$$p^2 = n(\pi)\ n(\alpha). \qquad (1)$$

We have two cases to consider

$$\text{A.}\ \begin{matrix} n(\pi) = p \\ n(\alpha) = p \end{matrix} \qquad \text{B.}\ \begin{matrix} n(\pi) = p^2 \\ n(\alpha) = 1 \end{matrix}$$

The case $n(\pi) = 1$ is excluded because the only numbers of $K(\sqrt{-3})$ whose norms are unity are the units.

A. From $n(\pi) = \pi\pi' = p$ and (1), it follows that $\alpha = \pi'$. From $n(\pi) = p$ we have $(a+b\rho)(a+b\rho^2) = a^2-ab+b^2 = p$, and since every positive rational prime, except 3, is of the form $3h+1$ or $3h-1$, it follows excluding the case $p = 3$, when $p = n(\pi)$,

$$a^2-ab+b^2 \equiv 1, \text{ mod } 3,$$
or
$$a^2-ab+b^2 \equiv -1, \text{ mod } 3.$$

The first of these congruences has the solutions

$$\begin{matrix} a = 0; & a = \pm 1; & a = 1; & a = -1 \\ b = \pm 1; & b = 0; & b = 1; & b = -1 \end{matrix} \text{, mod } 3,$$

while the second has no solutions.

Hence <u>when a positive rational prime other than 3 is the product of two conjugate primes of $K(\sqrt{-3})$, it has the form $3h+1$</u>.

The above fact is also expressed in the following manner: If a positive rational prime, p, other than 3, is the product of two conjugate primes of $K(\sqrt{-3})$, then $p \equiv 1$, mod 3.

When $p = 3$, we have

$$p = a^2-ab+b^2 = 3,$$

which is satisfied by

$$a = 1, \quad b = -1.$$

These values give

$$3 = (1-\rho)(1-\rho^2);$$

hence 3 is the product of two conjugate primes of $K(\sqrt{-3})$. These factors of 3 are, however, associated, for

$$1-\rho^2 = -\rho^2(1-\rho),$$

from which $3 = -\rho^2(1-\rho)(1-\rho) = -\rho^2(1-\rho)^2$, or $3 = -(\sqrt{-3})^2$; that is, 3 is associated with the square of a prime of $K(\sqrt{-3})$

B. From $n(\alpha) = 1$ it follows that α is a unit. Therefore p is associated with the prime π; that is p is a prime in $K(\sqrt{-3})$. When p is of the form $3h-1$, this case always occurs, for in order that a rational prime be factorable in $K(\sqrt{-3})$ it must either be 3 or of the form $3h+1$.

Using the notation of congruence we say that a rational prime p, when congruent to -1, mod 3, is always a prime in $K(\sqrt{-3})$.

We shall now show that every rational prime, p, of the form $3h+1$ can be resolved into the product of two conjugate primes of $K(\sqrt{-3})$.

Accepting the Law of Reciprocity of Quadratic Residues*, it follows that the congruence

$$X^2 = -3, \text{ mod } p, \quad p = 3h+1,$$

has roots; for

---

* Law of Reciprocity of Quadratic Residues: If p and q are two different positive odd primes, we have

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$$

The symbols (p/q) and (q/p) are equal if one at least of the two numbers, p and q, is of the form $4h+1$. These symbols are opposite in sign if both p and q are of the form $4h-1$.
If $p = 4h+1$ and $q = 4h+1$,
or $p = 4h+1$ and $q = 4h-1$, $(p/q)(q/p) = 1$
or $p = 4h-1$ and $q = 4h+1$,
While if $p = 4h-1$ and $q = 4h-1$, $(p/q)(q/p) = -1$

$$(-3/p) = (-1/p)(3/p),$$

if p is of the form $4h+1$

$$(-1/p) = 1, \text{ and } (3/p) = (p/3);$$

if p is of the form $4h-1$

$$(-1/p) = -1, \text{ and } (3/p) = -(p/3).$$

In either case we see therefore that

$$(-3/p) = (p/3) = (1/3) = 1.$$

Let a be a root; then

$$a^2 + 3 \equiv 0, \text{ mod } p, \quad p = 3h+1;$$

that is, $$(a+\sqrt{-3})(a-\sqrt{-3}) \equiv 0, \text{ mod } p.$$

Since $a+\sqrt{-3}$ and $a-\sqrt{-3}$ are integers of $K(\sqrt{-3})$, p must, if a prime in $K(\sqrt{-3})$, divide one of them; it follows then that either

$$a+\sqrt{-3} = p\,\frac{u+v\sqrt{-3}}{2} \qquad (2)$$

where u and v are both odd or both even, or

$$a-\sqrt{-3} = p\,\frac{u_1+v_1\sqrt{-3}}{2} \qquad (3)$$

where u and v are both odd or both even. (2) and (3) are, however, impossible, since $1/2\ pv = \pm 1$ implies that v is even, and hence that p is a divisor of 1, which is impossible.

We see therefore that p is not a prime in $K(\sqrt{-3})$ and, since the only way in which a rational prime is factorable in $K(\sqrt{-3})$ is into two conjugate primes, p is factorable in this manner. As in K(i) the primes of $K(\sqrt{-3})$ may be classified according to the rational primes of which they are factors as follows:

(1) <u>All positive rational primes of the form $3h+1$ are</u>

The symbol (a/p) was introduced by Legendre to indicate the quadratic character of an integer, a, with respect to a prime p. If (a/p) denotes +1, a is a quadratic residue of p; if (a/p) denotes -1, a is a quadratic non-residue of p.
Cahen: Theorie des Nombres. pp, 122— 136.
Reid: The Elements of the Theory of Algebraic Numbers. pp, 135—153.

factorable in $K(\sqrt{-3})$ into two conjugate primes.

(2) All positive rational primes of the form $3h-1$ are primes in $K(\sqrt{-3})$.

(3) The number 3 is associated with the square of a prime of the first degree.

The Unique Factorization Theorem for $K(\sqrt{-3})$

As in K(i) the proof of this theorem requires the proof of three fundamental theorems.

Theorem 1. If α be any integer of $K(\sqrt{-3})$, and β any integer of $K(\sqrt{-3})$ different from 0, there exists an integer γ of $K(\sqrt{-3})$ such that

$$n(\alpha - \gamma\beta) < n(\beta).$$

Let $\alpha/\beta = a + b\rho$, where $a = r + r_1$, $b = s + s_1$, r and s being the rational integers nearest to a and b respectively. It follows then that

$$|r_1| \leqq 1/2, \quad |s_1| \leqq 1/2.$$

We are able to show that $\gamma = r + s\rho$, will fulfil the required conditions of the theorem.

$$\alpha/\beta - \gamma = a + b\rho - \gamma = r_1 + s_1\rho.$$

$$n(\alpha/\beta - \gamma) = r_1^2 - r_1 s_1 + s_1^2 \leqq 3/4;$$

from which it follows that

$$n(\alpha/\beta - \gamma) < 1,$$

or multiplying by $n(\beta)$

$$n(\alpha - \gamma\beta) < n(\beta).$$

The following example will illustrate the theorem.

If $\alpha = 5 + 2\sqrt{-3}$, and $\beta = 1 + 3\sqrt{-3}$,

$$\frac{\alpha}{\beta} = \frac{5 + 2\sqrt{-3}}{1 + 3\sqrt{-3}} = \frac{23}{28} - \frac{13}{28}\sqrt{-3} = \frac{5}{14} - \frac{13}{14}\rho$$

and

$$\gamma = 1 - \rho = 1/2(3 - \sqrt{-3}).$$

Therefore $\alpha - \gamma\beta = 5+2\sqrt{-3} - 1/2(3-\sqrt{-3})(1+3\sqrt{-3}) = -2-2\sqrt{-3}$;

hence $n(-2-2\sqrt{-3}) = 16 < n(1+3\sqrt{-3})$.

Because the proofs of the two remaining theorems which lead to the unique factorization theorem together with the proof of that theorem itself are exactly similar to those in K(i) these theorems will merely be stated.

Theorem 2. If α and β be any two integers of $K(\sqrt{-3})$ prime to each other, there exist two integers, μ and ν, of $K(\sqrt{-3})$ such that

$$\alpha\mu + \beta\nu = 1.$$

Theorem 3. If the product of two integers, α and β of $K(\sqrt{-3})$ be divisible by a prime number, λ, at least one of the integers is divisible by λ.

The Unique Factorization Theorem. Every integer of $K(\sqrt{-3})$ can be represented in one and only one way as the product of prime numbers.

Chapter III

The Domain $K(\sqrt{2})$

The number $\sqrt{2}$ is defined by the equation

$$X^2-2=0$$

which it satisfies. It can be shown exactly as in K(i) that all numbers of $K(\sqrt{2})$ have the form $a+b\sqrt{2}$, where a and b are rational numbers. As in the preceding two domains every number, $\alpha = a+b\sqrt{2}$, of $K(\sqrt{2})$ satisfies a rational equation of the second degree. It can also be shown as in K(i) that the fundamental operations(division by 0 excluded) in this domain always give a number in the domain, and that these operations are in general unique.

The product $\alpha\alpha'$ as in the preceding domains is called the norm of α. In $n(\alpha) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2$ we notice the first important difference between this domain and the domains K(i) and $K(\sqrt{-3})$. While the norm of a number in either K(i) or $K(\sqrt{-3})$ is always a positive rational number in this domain the norm is not necessarily a positive rational number. It may be either a positive or negative rational number, depending on whether $2b^2$ is less or greater than a^2. This is the case of all quadratic domains defined by real numbers, while the norms of numbers of quadratic domains defined by imaginary numbers are always positive.

Algebraic Integers of $K(\sqrt{2})$

An algebraic integer of $K(\sqrt{2})$ is defined in the same manner as in $K(\sqrt{-3})$; that is, any algebraic number of $K(\sqrt{2})$ which satisfies an equation of the form

$$X^2+PX+Q=0$$

where P and Q are rational integers.

If we write all numbers of $K(\sqrt{2})$ in the form

$$\alpha = \frac{a_1 + b_1\sqrt{2}}{c_1},$$

where a_1, b_1, c_1 are rational integers having no common factor, although any two of them may have a common factor, we see that the necessary and sufficient conditions that α shall be an algebraic integer are

$$\alpha + \alpha' = \frac{a_1 + b_1\sqrt{2}}{c_1} + \frac{a_1 - b_1\sqrt{2}}{c_1} = \frac{2a_1}{c_1} = \text{a rational integer} \qquad (1)$$

$$\alpha\alpha' = \left(\frac{a_1 + b_1\sqrt{2}}{c_1}\right)\left(\frac{a_1 - b_1\sqrt{2}}{c_1}\right) = \frac{a_1^2 - 2b_1^2}{c_1^2} = \text{a rational integer} \qquad (2)$$

One at least of the three following cases must occur:

A. $c_1 \neq 2$ or 1; B. $c_1 = 2$: C, $c_1 = 1$.

A. If $c_1 \neq 2$ or 1, then by (1) a_1 and c_1 have a common factor which by virtue of (2) must be contained in b_1 also; for if a_1 is divisible by c_1 then a_1^2 is divisible by c_1^2. But $a_1^2 - 2b_1^2$ is also divisible by c_1^2, hence $2b_1^2$ must be divisible by c_1^2. Since $c_1 \neq 2$ or 1, b_1^2 must be divisible by c_1^2, and hence b_1 divisible by c_1; that is a_1, b_1, c_1 have a common factor.

B. If $c_1 = 2$, $2a_1/c_1$ may be an integer and a_1 and c_1 not have a common factor. But $a_1^2 - 2b_1^2$ must be divisible by c_1^2 or 4. If a_1 and b_1 are both even then a_1, b_1, c_1 have a common factor. We shall show that if a_1 and b_2 are both odd or one of them is even and the other odd that $a_1^2 - 2b_1^2$ is not divisible by c_1^2 or 4. First let them both be odd; then we may write them in the form

$$a_1 = 2k_1 \pm 1,$$
$$b_1 = 2k_2 \pm 1.$$

Then $$a_1^2 - 2b_1^2 = 4(k_1^2 \pm k_1) - 8(k_2^2 \pm k_2) - 1.$$

We see readily that this expression when divided by 4 does not give a rational integer.

Now let a_1 be even and b_1 odd; then we may write them in the

form

$$a_1 = 2k_1$$
$$b_1 = 2k_2 \pm 1.$$

Then $a_1^2 - 2b_1^2 = 4k_1^2 - 8(k_2^2 \pm k_2) - 2$; and we see that this expression does not reduce to a rational integer when divided by 4.

Now let a_1 be odd and b_1 even; then we may write them in the form

$$a_1 = 2k_1 \pm 1$$
$$b_1 = 2k_2.$$

Then $a_1^2 - 2b_1^2 = 4(k_1^2 \pm k_1) + 1 - 8k_2^2$; and neither does this expression give a rational integer when divided by 4.

Hence case C is the only one which is satisfied, that is $c_1 = 1$.

Therefore all integers of $K(\sqrt{2})$ have the form $a + b\sqrt{2}$, where a and b are rational integers, and all numbers of this form of $K(\sqrt{2})$ are rational integers.

Prime Numbers of $K(\sqrt{2})$

The definitions of prime and composite number are the same as those in the preceding domains, and we can employ the same methods to determine whether or not an integer of $K(\sqrt{2})$ is prime or composite. A unit of $K(\sqrt{2})$ is defined in the same manner as in $K(1)$ and in $K(\sqrt{-3})$, but they may also be defined as those integers of $K(\sqrt{2})$ whose norms are 1 or -1. We note here then another very striking difference between this domain and the preceding domains; for while the number of units in the latter were finite in number, the number of units in this domain is infinite. For if we have $\theta = a + b\sqrt{2}$, a unit of $K(\sqrt{2})$, we have

$$n(\theta) = 1 \text{ or } n(\theta) = -1,$$

that is $a^2 - 2b^2 = 1$ or $a^2 - 2b^2 = -1$.

Since an infinite number of solutions can be found for these equations, we are able to represent $a + b\sqrt{2}$ in an infinite number of ways. We may then represent every unit of $K(\sqrt{2})$ as $\pm(a + b\sqrt{2})^n$

where n is a positive or negative rational integer or 0.

We could have expressed the units of K(i) in a similar manner, but (i) gives only four numbers, 1, -1, i and -i, since $i^4 = 1$. In a similar manner we could have expressed the units of $K(\sqrt{-3})$ in the form $\pm\rho^n$, but $\pm\rho^n$ gives only six different numbers, 1, -1, ρ, $-\rho$, ρ^2 and $-\rho^2$, since $\rho^3 = 1$.

Ex. 1. To determine whether $1+2\sqrt{2}$ is a prime or composite number of $K(\sqrt{2})$.

Put $$1+2\sqrt{2} = (a+b\sqrt{2})(c+d\sqrt{2}),$$

then $$-7 = (a^2-2b^2)(c^2-2d^2).$$

We then have either

$$a^2-2b^2 = -7, \qquad c^2-2d^2 = 1, \tag{1}$$

or

$$a^2-2b^2 = 1, \qquad c^2-2d^2 = -7. \tag{2}$$

From (2) it follows that $a+b\sqrt{2}$ is a unit, and from (1) it follows that $c+d\sqrt{2}$ is a unit. Therefore $1+2\sqrt{2}$ is not decomposable into two factors in $K(\sqrt{2})$, both of which are different from unity and is hence a prime number in $K(\sqrt{2})$.

Ex. 2. To determine whether $2+3\sqrt{2}$ is a prime or composite number of $K(\sqrt{2})$.

Put $$2+3\sqrt{2} = (a+b\sqrt{2})(c+d\sqrt{2}),$$

then $$-14 = (a^2-2b^2)(c^2-2d^2).$$

We then have either

$$a^2-2b^2 = 1, \qquad c^2-2d^2 = -14, \tag{3}$$

or

$$a^2-2b^2 = 2, \qquad c^2-2d^2 = -7, \tag{4}$$

or

$$a^2-2b^2 = -2, \qquad c^2-2d^2 = 7. \tag{5}$$

From (3) it follows that $a+b\sqrt{2}$ is a unit, but (4) gives the following solutions

$$a = \pm 2, \quad b = \pm 1, \quad c = \pm 1, \quad d = \pm 2,$$

which give

$$2+3\sqrt{2} = (2+\sqrt{2})(-1+2\sqrt{2}) = (-2-\sqrt{2})(1-2\sqrt{2}),$$

the proper factors being selected by trial.

As solutions of (5) we have

$$a = \pm 4, \quad b = \pm 3, \quad c = \pm 5, \quad d = \pm 3,$$

which give

$$2+3\sqrt{2} = (4+3\sqrt{2})(5-3\sqrt{2}) = (-4-3\sqrt{2})(-5+3\sqrt{2}),$$

the proper factors being selected by trial.

Classification of the Prime Numbers of $K(\sqrt{2})$

By the same method of reasoning employed in $K(i)$, it becomes evident that every prime, π, of $K(\sqrt{2})$ is a divisor of one and only one rational prime. Therefore in order to obtain all primes of $K(\sqrt{2})$ it is only necessary to resolve all positive rational primes considered as integers of $K(\sqrt{2})$ into their prime factors in $K(\sqrt{2})$.

If we let $\pi = a+b\sqrt{2}$, be any prime of $K(\sqrt{2})$ and p the positive rational prime of which π is the divisor, we have

$$p = \pi\alpha,$$

and hence

$$p^2 = n(\pi)\, n(\alpha) \qquad (1)$$

We then have two cases to consider:

A. $n(\pi) = p$, $n(\alpha) = p$ B. $n(\pi) = p^2$, $n(\alpha) = 1$.

The case $n(\pi) = 1$ is excluded because the only numbers of $K(\sqrt{2})$ whose norms give unity are the units of $K(\sqrt{2})$.

A. From $n(\pi) = \pi\pi' = p$ and (1) it follows that $\alpha = \pi'$. Since every rational prime, except 2, is of one of the forms, $8h \pm 1$, $8h \pm 3$, it follows (excluding the case $p = 2$) when

$$p = n(\pi),$$

that $a^2 - 2b^2 \equiv 1, \mod 8, \qquad (2)$
or $a^2 - 2b^2 \equiv -1, \mod 8, \qquad (3)$
or $a^2 - 2b^2 \equiv 3, \mod 8, \qquad (4)$
or $a^2 - 2b^2 \equiv -3, \mod 8, \qquad (5)$

The congruence (2) has the solutions

$$\begin{array}{llllll} a = \pm 1, & \pm 1, & \pm 3, & \pm 3, & \mod 8. \\ b = \pm 2, & 0, & \pm 2, & 0, & \end{array}$$

The congruence (3) has the solutions

$$\begin{matrix} a = \pm 1, & \pm 1, & \pm 3, & \pm 3 \\ b = \pm 1, & \pm 3, & \pm 1, & \pm 3 \end{matrix} \quad , \text{ mod } 8.$$

(4) and (5) have no solutions, for they give

$$a^2 \equiv 2b^2 \pm 3, \text{ mod } 8,$$

and hence require that $2b^2 \pm 3$ shall be a quadratic residue of 8. But the only quadratic residues of 8 are 1 and 4. It follows then that a necessary condition that (4) and (5) shall have a solution is

$$1 \equiv 2b^2 \pm 3, \text{ mod } 8, \text{ or } 4 \equiv 2b^2 \pm 3, \text{ mod } 8.$$

These congruences give

$$2b^2 \equiv 4 \text{ or } -2, \text{ mod } 8, \tag{6}$$

and

$$2b^2 \equiv 1 \text{ or } 7, \text{ mod } 8. \tag{7}$$

It is easily seen that no value of b will satisfy either (6) or (7). Hence (4) and (5) have no solutions.

Therefore <u>when a positive rational prime other than 2 is the product of two conjugate primes of $K(\sqrt{2})$, it has the form $8h \pm 1$</u>.

When p = 2, we have

$$a^2 - 2b^2 = 2, \quad c^2 - 2d^2 = 2.$$

This equation is satisfied by $a = \pm 2$, $b = \pm 1$, $c = \pm 2$, $d = \pm 1$. Hence $2 = (a + b\sqrt{2})(c + d\sqrt{2}) = (2 + \sqrt{2})(2 - \sqrt{2}) = (1 + \sqrt{2})(-1 + \sqrt{2})(\sqrt{2})^2$; that is, <u>2 is associated with the square of a prime of $K(\sqrt{2})$</u>.

B. Since $n(\alpha) = 1$, α is a unit. Therefore p is associated with the prime π; that is, p is a prime in $K(\sqrt{2})$. When p is of the form $8h \pm 3$ this case always occurs, for we have just seen that to be factorable in $K(\sqrt{2})$ a rational prime must be either 2 or of the form $8h \pm 1$. We can express the above fact also in the following manner: A rational prime, p, when congruent to ± 3, mod 8, is always a prime in $K(\sqrt{2})$.

We shall now show that every rational prime, p, of the form $8h \pm 1$ can be resolved into the product of two conjugate primes of

$K(\sqrt{2})$.

The congruence $X^2 \equiv 2, \text{ mod } p, \; p = 8h \pm 1$, has roots, for $(2/p) = 1$ when $p = 8h \pm 1$.

Let a be a root, then $a^2 \equiv 2, \text{ mod } p,$

that is $(a+\sqrt{2})(a-\sqrt{2}) \equiv 0, \text{ mod } p.$

Since $a+\sqrt{2}$ and $a-\sqrt{2}$ are both integers of $K(\sqrt{2})$, p, if a prime of $K(\sqrt{2})$ must divide either $a+\sqrt{2}$ or $a-\sqrt{2}$. We shall see that this is impossible, for from

$$a \pm \sqrt{2} = p(c+d\sqrt{2}),$$

where $c+d\sqrt{2}$ is an integer of $K(\sqrt{2})$, it would follow that

$$pd = \pm 1,$$

which is impossible, since p and d are both rational integers and $p > 1$. Hence p is not a prime in $K(\sqrt{2})$, and since we have seen that the only way in which a rational prime can be factored in $K(\sqrt{2})$ is into two conjugate prime factors, p is factorable in this manner.

As in K(i) and in $K(\sqrt{-3})$ the primes of $K(\sqrt{2})$ may be classified according to the rational primes of which they are factors as follows:

(1) <u>All positive rational primes of the form $8h \pm 1$ are factorable in $K(\sqrt{2})$ into two conjugate primes of $K(\sqrt{2})$</u>.

(2) <u>All positive rational primes of the form $8h \pm 3$ are primes in $K(\sqrt{2})$</u>.

(3) <u>The number 2 is associated with the square of a prime of the first degree in $K(\sqrt{2})$</u>.

<u>The Unique Factorization Theorem for $K(\sqrt{2})$</u>

As in K(i) and in $K(\sqrt{-3})$ the proof of this theorem requires the proof of three fundamental theorems. The proofs of these

theorems and of the unique factorization theorem itself are identical with those in K(i) and $K(\sqrt{-3})$ with the exception that the absolute value of the norm is substituted for the value of the norm of an integer. This is necessary when we make a comparison between two integers of $K(\sqrt{2})$ similar to that made between rational integers when we say that one is greater in absolute value than the other. In K(i) and $K(\sqrt{-3})$ the norms of all numbers were positive and hence were their own absolute values.

Theorem 1. *If α be any integer of $K(\sqrt{2})$, and β any integer of $K(\sqrt{2})$ different from 0, there exists an integer, γ, of $K(\sqrt{2})$ such that*

$$|n(\alpha-\gamma\beta)|<|n(\beta)|.$$

Let $$\alpha/\beta = a+b\sqrt{2},$$

where $a = r+r_1$, $b = s+s_1$, r and s being the rational integers nearest to a and b respectively. It follows then that

$$|r_1| \leqq 1/2, \qquad |s_1| \leqq 1/2.$$

We are able to show that $\gamma = r+s\sqrt{2}$, will fulfil the required conditions of the theorem.

Since $$\alpha/\beta - \gamma = a+b\sqrt{2}-\gamma = r_1+s_1\sqrt{2},$$

then $|n(\alpha/\beta-\gamma)| = |r_1^2-2s_1^2| \leqq 1/4$, and it follows therefore that $|n(\alpha/\beta-\gamma)|<1$.

Multiplying by $n(\beta)$, we obtain

$$|n(\alpha-\gamma\beta)|<|n(\beta)|.$$

The following example will illustrate the theorem.

If $\alpha = 5+2\sqrt{2}$, and $\beta = 1+3\sqrt{2}$, then

$$\frac{\alpha}{\beta} = \frac{5+2\sqrt{2}}{1+3\sqrt{2}} = \frac{-7}{-17}+\frac{13}{17}\sqrt{2}$$

and $$\gamma = 1+\sqrt{2}.$$

$$\alpha - \gamma\beta = (5+2\sqrt{2}) - (1+\sqrt{2})(1+3\sqrt{2}) = -2-3\sqrt{2}.$$

$$|n(\alpha-\gamma\beta)| = |n(-2-3\sqrt{2})| = 14 < |n(1+3\sqrt{2})|.$$

For similar considerations as stated in $K(\sqrt{-3})$ the two remaining theorems and the unique factorization theorem itself will merely be stated.

Theorem 2. *If α and β be any two integers of $K(\sqrt{2})$ prime to each other there exist two integers, μ and ν, such that*

$$\alpha\mu + \beta\nu = 1.$$

Theorem 3. *If the product of two integers, α and β, of $K(\sqrt{2})$ be divisible by a prime number, λ, at least one of the integers is divisible by λ.*

The Unique Factorization Theorem. Every integer of $K(\sqrt{2})$ can be represented in one and only one way as the product of prime numbers.

Chapter IV

The Domain $K(\sqrt{-5})$

The number $\sqrt{-5}$ is defined by the equation

$$X^2+5 = 0,$$

which it satisfies. It can be shown exactly as in K(i) that all numbers of $K(\sqrt{-5})$ have the form $a+b\sqrt{-5}$, where a and b are rational numbers. As in the preceding domains every number, $\alpha = a+b\sqrt{-5}$ of $K(\sqrt{-5})$ satisfies a rational equation of the second degree. It can also be shown as in K(i) that the fundamental operations (division by 0 excluded) in this domain always give a number in the domain, and that these operations are in general unique.

The norm of α, $= a+b\sqrt{-5}$ equals a^2+5b^2, is always a positive number, agreeing in this respect with the norms of numbers of K(i) and $K(\sqrt{-3})$.

Algebraic Integers of $K(\sqrt{-5})$

An algebraic integer of $K(\sqrt{-5})$ is defined in the same manner as in $K(\sqrt{-3})$; that is, an algebraic integer of $K(\sqrt{-5})$ is any algebraic number of $K(\sqrt{-5})$ which satisfies an equation of the form

$$X^2+PX+Q = 0$$

where P and Q are rational integers.

If we write all numbers of $K(\sqrt{-5})$ in the form

$$\alpha = \frac{a_1+b_1\sqrt{-5}}{c_1},$$

where a_1, b_1, c_1 are rational integers having no common factor, although any two of them may have a common factor, we see that the necessary and sufficient conditions that α shall be an algebraic integer are

$$\alpha+\alpha' = \frac{a_1+b_1\sqrt{-5}}{c_1} + \frac{a_1-b_1\sqrt{-5}}{c_1} = \frac{2a_1}{c_1} = \text{a rational integer} \quad (1)$$

$$\alpha\alpha' = \left(\frac{a_1+b_1\sqrt{-5}}{c_1}\right)\left(\frac{a_1-b_1\sqrt{-5}}{c_1}\right) = \frac{a_1^2+5b_1^2}{c_1^2} = \text{a rational integer} \qquad (2)$$

One at least of the three following cases must occur:

A. $c_1 \neq 2$ or 1; B. $c_1 = 2$; C. $c_1 = 1$.

A. If $c_1 \neq 2$ or 1, then by (1) a_1 and c_1 have a common factor which we shall show by virtue of (2) is contained in b_1 also. Since a_1 is divisible by c_1, a_1^2 is divisible by c_1^2. But $a_1^2+5b_1^2$ must also be divisible by c_1^2; therefore $5b_1^2$ must be divisible by c_1^2. Since $c_1 \neq 2$ or 1, b_1^2 must be divisible by c_1^2, that is, b_1 must be divisible by c_1.

B. If $c_1 = 2$, $2a_1/c_1$ may be an integer and a_1 and c_1 have no common factor. We shall show that $a_1^2+5b_1^2$ is not divisible by c_1^2 or 4 unless a_1 and b_1 are both even, that is, unless a_1, b_1, c_1 have the common factor 2. If a_1 is odd and b_1 even we may write them in the form

$$a_1 = 2k_1 \pm 1$$
$$b_1 = 2k_2$$

Then $a_1^2+5b_1^2 = 4(k_1^2 \pm k_1) + 1 + 20k_2^2$ We see that this expression does not give a rational integer when divided by 4.

If a_1 is even and b_1 odd we may write them in the form

$$a_1 = 2k_1$$
$$b_1 = 2k_2 \pm 1.$$

Then $a_1^2+5b_1^2 = 4k_1^2+20(k_2^2 \pm k_2)+5$. This expression does not reduce to a rational integer when divided by 4.

If a_1 and b_1 are both odd we may write them in the form

$$a_1 = 2k_1 \pm 1,$$
$$b_1 = 2k_2 \pm 1.$$

Then $a_1^2+5b_1^2 = 4(k_1^2 \pm k_1) + 20(k_2^2 \pm k_2) + 6$. This expression does not give a rational integer when divided by 4.

Hence C is the only admissible case, that is, $c_1 = 1$.

Therefore all integers of $K(\sqrt{-5})$ have the form $a+b\sqrt{-5}$, where a and b are rational integers, and all numbers of this form

of $K(\sqrt{-5})$ are rational integers.

Prime Numbers of $K(\sqrt{-5})$

The definitions of prime and composite number are identical with those in the preceding domains; and we can employ the same methods to determine whether or not an integer of $K(\sqrt{-5})$ is prime or composite. Since the norms of all numbers of $K(\sqrt{-5})$ are positive it can be easily shown that the units of $K(\sqrt{-5})$ are 1 and -1. If $\theta = a + b\sqrt{-5}$, is a unit of $K(\sqrt{-5})$ then

$$n(\theta) = a^2 + 5b^2 = 1.$$

The only integral values of a and b which satisfy this equation are

$$b = 0, \quad a = \pm 1.$$

Therefore 1 and -1 are the only numbers of $K(\sqrt{-5})$ whose norms give +1, and hence are the only units of $K(\sqrt{-5})$.

The associated integers of $K(\sqrt{-5})$ are therefore α and $-\alpha$, obtained by multiplying any integer, α, by the units of $K(\sqrt{-5})$.

Ex. 1. To determine whether 3 is a prime or composite number of $K(\sqrt{-5})$.

Put $$3 = (a + b\sqrt{-5})(c + d\sqrt{-5});$$

then $$9 = (a^2+5b^2)(c^2+5d^2).$$

We then have either

$$a^2+5b^2 = 3, \quad c^2+5d^2 = 3, \tag{1}$$

or

$$a^2+5b^2 = 9, \quad c^2+5d^2 = 1, \tag{2}$$

We see then that (1) is impossible since a, b, c and d are to be rational integers. From (2) it follows that $c + d\sqrt{-5}$ is a unit. Hence 3 is a prime number in $K(\sqrt{-5})$.

Ex. 2. To determine whether $1 + 4\sqrt{-5}$ is a prime or composite number of $K(\sqrt{-5})$.

Put $$1 + 4\sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5});$$

then $$81 = (a^2+5b^2)(c^2+5d^2).$$

We then have either

$$a^2+5b^2 = 81, \qquad c^2+5d^2 = 1, \tag{3}$$

or
$$a^2+5b^2 = 27, \qquad c^2+5d^2 = 3, \tag{4}$$

or
$$a^2+5b^2 = 9, \qquad c^2+5d^2 = 9, \tag{5}$$

From (3) it follows that $c+d\sqrt{-5}$ is a unit. Equation (4) is evidently impossible for we have assumed that c and d are rational integers. As solutions of (5) we have

$$a = \pm 2, \qquad c = \pm 2,$$
$$b = \pm 1, \qquad d = \pm 1,$$

from which it follows that

$$1+4\sqrt{-5} = (2-\sqrt{-5})(-2+\sqrt{-5}),$$

the proper factors being selected by trial. Since neither $2-\sqrt{-5}$ nor $-2+\sqrt{-5}$ is a unit in $K(\sqrt{-5})$ we see that $1+4\sqrt{-5}$ is a composite number of $K(\sqrt{-5})$.

Failure of the Unique Factorization Theorem for $K(\sqrt{-5})$

The main reason for the introduction of a discussion of this domain was to show that the unique factorization theorem breaks down for integers of $K(\sqrt{-5})$, and that this failure makes necessary the introduction of the conception of ideal numbers.

We shall try to establish the unique factorization theorem for this domain in a manner analogous to that pursued in the preceding domains, that is, we shall try to establish for $K(\sqrt{-5})$ the three fundamental theorems necessary for the proof of the unique factorization theorem.

Theorem 1. If α be any integer of $K(\sqrt{-5})$ and β any integer of $K(\sqrt{-5})$ different from 0, there exists an integer γ of $K(\sqrt{-5})$ such that

$$n(\alpha-\gamma\beta) < n(\beta).$$

Let $\alpha/\beta = a+b\sqrt{-5},$

where $a = r+r_1, \qquad b = s+s_1,$

r and s being the rational integers nearest to a and b respectively, and hence it follows that

$$|r_1| \leq 1/2, \qquad |s_1| \leq 1/2$$

As in the preceding domains, let

$$\gamma = r + s\sqrt{-5};$$

whence

$$n(\alpha/\beta - \gamma) = r_1^2 + 5s_1^2 \leq 6/4,$$

that is, when γ is determined as in the preceding domains, we may have in $K(\sqrt{-5})$

$$n(\alpha/\beta - \gamma) > 1 \text{ instead of } < 1$$

as has been the case in the three preceding domains. Therefore the integer γ chosen in this manner will not necessarily satisfy the requirements of the theorem. The above method therefore fails. We are able to show by a specific example that this theorem does fail for some integers of $K(\sqrt{-5})$.

Let $\alpha = 2$ and $\beta = 1 - \sqrt{-5}$,

then

$$\frac{\alpha}{\beta} = \frac{2}{1-\sqrt{-5}} = \frac{1-\sqrt{-5}}{3}$$

Our task is to find an integer $\gamma = c + d\sqrt{-5}$, such that

$$n(\alpha/\beta - \gamma) < 1.$$

But

$$n(\alpha/\beta - \gamma) = n(1/3 - 1/3\sqrt{-5} - c - d\sqrt{-5})$$
$$= (1/3 - c)^2 + 5(-1/3 - d)^2.$$

We must therefore find integral values of c and d such that

$$(1/3 - c)^2 + 5(-1/3 - d)^2 < 1.$$

We see at once this is impossible for since c and d can not both be zero, this expression can never be less than 1. Suppose that d = 0, then the least possible value that c can assume is 1. If d = 0 and c = 1, the expression

$$(1/3 - c)^2 + 5(-1/3 - d)^2 = 1.$$

If c = 0 and d = 1, the expression

$$(1/3 - c)^2 + 5(-1/3 - d)^2 = 9.$$

We see then that the method of proof adopted for Theorem 1 depends upon the general form of the norm of a number r_1+s_1u, where 1, u is a basis* of the domain. Thus in K(i), $K(\sqrt{-3})$, $K(\sqrt{2})$ and $K(\sqrt{-5})$ we have respectively

$$\left|n(r_1+s_1u)\right| = \left|r_1^2+s_1^2\right|, \quad \left|r_1^2-r_1s_1+s_1^2\right|, \quad \left|r_1^2-2s_1^2\right|, \text{ and } \left|r_1^2+5s_1^2\right|,$$

and the method is successful if

$$|r_1| \leqq 1/2, \qquad |s_1| \leqq 1/2$$

be a sufficient condition for

$$\left|n(r_1+s_1u)\right| < 1,$$

Which we have noted is the case in K(i), $K(\sqrt{-3})$ and $K(\sqrt{2})$ but not in $K(\sqrt{-5})$.

Theorem 2. *If α and β be any two integers of $K(\sqrt{-5})$, prime to each other, there exist two integers, u and v of $K(\sqrt{-5})$ such that*

$$\alpha u+\beta v = 1.$$

We saw in K(i) that the proof of this theorem is based upon Theorem 1. which we have just seen does not hold for $K(\sqrt{-5})$. This does not, however, justify the assumption that Theorem 2 does not hold for $K(\sqrt{-5})$. We are able to show by the following example that Theorem 2 does not hold in general for the integers of $K(\sqrt{-5})$.

Let $\alpha = 2$ and $\beta = 1-\sqrt{-5}$. It can be easily shown that 2 and $1-\sqrt{-5}$ are prime numbers of $K(\sqrt{-5})$; moreover they are not associates. Hence they are prime to each other. The theorem breaks down unless we are able to find two integers, $u = c+d\sqrt{-5}$, and $v = e+f\sqrt{-5}$, such that

$$\alpha u+\beta v = 1. \tag{6}$$

If $$2(c+d\sqrt{-5})+(1-\sqrt{-5})(e+f\sqrt{-5}) = 1,$$

it follows that $2c+e+5f = 1$
and $2d-e+f = 0,$
from which it follows $2c+2d+6f = 1.$ (7)

* Two numbers, u_1, u_2 are said to form a basis of a domain if every

(7) is impossible because only the left member of the equation is divisible by 2, and c, d and f are rational integers. Therefore μ and ν can not be found so as to satisfy (6) and we see that the theorem does not hold in general for the integers of $K(\sqrt{-5})$.

Theorem 3. *If the product of two integers, α and β of $K(\sqrt{-5})$ is divisible by a prime number, λ, at least one of the integers is divisible by λ.*

This theorem which is a necesary as well as sufficient condition for the unique factorization theorem as we have seen in K(i), requires Theorem 2 as a necessary condition for its validity. Since Theorem 2 does not hold in general for the integers of $K(\sqrt{-5})$ Theorem 3 does not hold either. We are able to show by the following example that this theorem, and consequently the unique factorization also, does not hold in general for the integers of $K(\sqrt{-5})$.

$$9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}).$$

We have shown that 3 is a prime number of $K(\sqrt{-5})$* ; in a similar manner it can be shown easily that $2+\sqrt{-5}$ and $2-\sqrt{-5}$ are also prime numbers of $K(\sqrt{-5})$. The factors of one product are not associated with the factors of the other. Therefore 9 is represented in two different ways as the product of prime factors.

This failure of the unique factorization theorem does not occur in $K(\sqrt{-5})$ alone. If we examine the domain $K(\sqrt{-23})$ we see that

$$27 = 3\cdot 3\cdot 3 = (2+\sqrt{-23})(2-\sqrt{-23}),$$

and by the same methods employed in the other domains we are able to show that 3, $2+\sqrt{-23}$ and $2-\sqrt{-23}$ are prime numbers of $K(\sqrt{-23})$.

---

integer of the domain can be represented in the form $a_1u_1+a_2u_2$, where a_1 and a_2 are rational integers.

* p, 41

The Introduction of the Ideal

Now that we have seen that the unique factorization theorem breaks down for the integers of $K(\sqrt{-5})$, we are confronted with the question: is it possible, by the introduction of a new kind of number, to reestablish this important theorem for the integers of $K(\sqrt{-5})$. We shall show that the introduction of the ideal number will accomplish this fact, the primes of $K(\sqrt{-5})$ being no longer considered as primes but as being factorable into these ideal numbers.

The nature of these ideal numbers will be understood better if we consider the narrowed number domain consisting of all positive rational integers congruent to 1, mod 5; that is,

$$1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, \ldots\ldots \quad (8)$$

We shall see that if we consider our definition of prime number the same as in $K(i)$, when our operations are confined to numbers of this domain, the unique factorization theorem does not in general hold; for example,

$$546 = 6 \cdot 91 = 21 \cdot 26,$$
$$3726 = 6 \cdot 621 = 81 \cdot 46,$$

The numbers, 6, 21, 26, 46, 81, 91 and 621 are easily seen by multiplication of the numbers (8) to be prime in this domain. The cause of this failure of the unique factorization theorem is due to the absence of the remaining positive integers. If we suppose that these integers do not exist, in order to reestablish the unique factorization theorem we must introduce symbols which have the properties of these missing integers in so far as our special problem is concerned. Let us consider

$$546 = 6 \cdot 91 = 21 \cdot 26.$$

Since 6 is not contained in either 21 or 26 although the product $21 \cdot 26$ is divisible by 6, we can suppose 6 to be the product of two

factors one of which is contained in 21 , the other in 26, and denote these factors by (6, 21) and (6, 26) respectively. In this sense we can therefore consider (6, 21) as the greatest common divisor of 6 and 21. Similarly we consider (6, 26) as the greatest common divisor of 6 and 26.

We are able then to write

$$6 = (6, 21)(6, 26),$$

denoting by this equation that every integer which is divisible by 6 is divisible by (6, 21)(6, 26) and conversely. Similarly we have

$$\begin{aligned} 91 &= (91, 21)(91, 26), \\ 21 &= (21, 6)(21, 91), \\ 26 &= (26, 6)(26, 91). \end{aligned}$$

As a consequence of these representations we have

$$\begin{aligned} 546 &= 6 \cdot 91 = (6, 21)(6, 26)(91, 21)(91, 26) \\ &= 21 \cdot 26 = (21, 6)(21, 91)(26, 6)(26, 91). \end{aligned}$$

These two factorizations are seen to be the same since a change in the order of the numbers in the parenthesis has no effect on the symbol; that is, (6, 21) = (21, 6), etc.

We see from the above discussion that the failure of the unique factorization theorem in a certain number domain can be remedied by the introduction of a new kind of number, each of which is defined by a pair of integers of the domain and may be looked upon as the greatest common divisor of the integers. These new numbers, called ideal numbers, which we shall introduce into the domain $K(\sqrt{-5})$ in order to reestablish the unique factorization theorem, will be defined as each <u>being the greatest common divisor of an infinite system of integers of $K(\sqrt{-5})$ and as defined by any finite number of these integers such that all other integers of the system are linear combinations of these with coefficients which are integers of the domain</u>.

If we consider the equation

$$9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}),$$

we see that since 3 divides neither $(2+\sqrt{-5})$ nor $(2-\sqrt{-5})$, although it divides their product, in order to reestablish the unique factorization theorem for the integers of $K(\sqrt{-5})$ we shall have to consider 3 as the product of two ideal factors, $\underline{a}^*$ and $\underline{b}$, which divide $2+\sqrt{-5}$ and $2-\sqrt{-5}$ respectively, the quotients being supposed to be ideal numbers also. We can denote $\underline{a}$ and $\underline{b}$ respectively by the symbols $(3, 2+\sqrt{-5})$ and $(3, 2-\sqrt{-5})$. If we consider $\underline{a}$ to be the greatest common divisor of 3 and $2+\sqrt{-5}$, it will bear that same relation to the entire system of integers, which are linear combinations of 3 and $2+\sqrt{-5}$; that is, those of the form $3\alpha + (2+\sqrt{-5})\beta$, where α and β are any integers of the domain. Conversely we have, if $\underline{a}$ bears this relation to the entire system it will bear it to 3 and $2+\sqrt{-5}$.

Hence we may write

$$\underline{a} = (3, 2+\sqrt{-5}),$$

meaning by this symbol the entire system of integers which are linear combinations of 3 and $2+\sqrt{-5}$, with coefficients which are integers of the domain.

In a similar manner we write

$$\underline{b} = (3, 2-\sqrt{-5}).$$

We are now in a position to show that although the factorization of 9 into prime factors in $K(\sqrt{-5})$ is not unique, nevertheless when we resolve the principal ideal** $\underline{9}$ into its prime ideal***

---

* Ideal numbers will be written thus $\underline{a}$, $\underline{b}$.

** $\underline{a}$ is defined as a principal ideal if among the numbers of $\underline{a}$ there exist a number, α, such that all numbers of the ideal are multiples of α.

*** A prime ideal is defined as an ideal different from $\underline{1}$ and divisible only by itself and $\underline{1}$.

factors this factorization is unique.

$$\underline{9} = \underline{3}\cdot\underline{3} = (2+\sqrt{-5})(2-\sqrt{-5}); \qquad (9)$$

$$\underline{3} = (3,\ 2+\sqrt{-5})(3,\ 2-\sqrt{-5}),$$

$$2+\sqrt{-5} = (2+\sqrt{-5},\ 3)(2+\sqrt{-5},\ 3),$$

$$2-\sqrt{-5} = (2-\sqrt{-5},\ 3)(2-\sqrt{-5},\ 3).$$

The factors $\underline{3}$, $(2+\sqrt{-5})$ and $(2-\sqrt{-5})$ are all prime ideals of $K(\sqrt{-5})$. Substituting in (9) we have

$$\underline{9} = \underline{3}\cdot\underline{3} = (3,\ 2+\sqrt{-5})(3,\ 2-\sqrt{-5})(3,\ 2+\sqrt{-5})(3,\ 2-\sqrt{-5})$$
$$= (3,\ 2+\sqrt{-5})^2(3,\ 2-\sqrt{-5})^2.$$

$$\underline{9} = (2+\sqrt{-5})(2-\sqrt{-5}) = (2+\sqrt{-5},\ 3)(2+\sqrt{-5},\ 3)(2-\sqrt{-5},\ 3)(2-\sqrt{-5},\ 3)$$
$$= (2+\sqrt{-5},\ 3)^2(2-\sqrt{-5},\ 3)^2.$$

These two factorizations are identical; hence we see that $\underline{9}$ can be factored in one and only one way into prime ideal factors.

We have now shown that the introduction of the ideal number reestablishes the unique factorization theorem for $K(\sqrt{-5})$, at least in the specific example given. We shall make no effort to prove the general theorems leading to the unique factorization theorem and the unique factorization theorem itself in terms of these ideal numbers, but the proofs are exactly analogous to the proofs of these theorems in the preceding domains. These proofs are given in detail in such works on the theory of algebraic numbers as Reid's " The Elements of the Theory of Algebraic Numbers" and Hilbert's "Theorie des Corps de Nombres Algebriques".

The introduction of ideal factors is due to Kummer, but the form used in this paper and known as ideals is due to Dedekind. Reid: The Elements of the Theory of Algebraic Numbers, p.267.

Chapter V

Finite Domains with respect to certain Prime and Double Moduli

The domains which we have considered so far in this paper have contained an infinite number of numbers. The domains considered in this chapter contain only a finite number of numbers.

Domain with respect to the Prime Modulus, 13

If we consider only numbers less than our modulus then the numbers of this domain are

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12.$$

The most general set of numbers of this domain is written

$$kp,\ kp \pm 1,\ kp \pm 2,\ kp \pm 3,\ kp \pm 4,\ kp \pm 5,\ kp \pm 6,$$

where p is our modulus and $k = 0, 1, 2, \ldots\ldots, n$.

We shall show that this set of numbers satisfies our definition of a domain of rationality; that is, that the fundamental operations, addition, subtraction, multiplication and division (division by 0 excluded) in this set of numbers always give a number in the set. Moreover we shall find that these operations are in general unique. No two numbers of the above set are equal.

It is obvious that if we add any two numbers of the set we will obtain another number of the set, mod 13; that the operation is unique is seen from the following:

If x, y and z are three numbers of the set so related that

$$x+y \equiv z, \text{ mod } 13,$$

and if we also have $x+y_1 \equiv z$, mod 13, where y_1 is another integer of the set different from y, it would follow that $y = y_1$. But this is contrary to the hypothesis that no two numbers of the set

are equal. Hence we see that the process of addition in this domain is unique.

In a similar manner one is able to show that the process of subtraction in this domain is also unique.

If we have three integers, x, y, z, of the set so related that

$$xy \equiv z, \text{ mod } 13 \quad (x, y \text{ and } z \neq 0)$$

it can be easily shown that there is no other integer in the set by which x can be multiplied so as to give z, mod 13. Suppose that there is such an integer, say y_1, and we have

$$xy_1 \equiv z, \text{ mod } 13.$$

From these two congruences it follows that

$$x(y-y_1) \equiv 0, \text{ mod } 13.$$

This congruence is impossible*unless $x \equiv 0$ or $y-y_1 \equiv 0$; but we started out with the assumption that $x \neq 0$, therefore $y-y_1 \equiv 0$, that is $y = y_1$. We see then that multiplication is unique.

The fact that if we divide one integer of this domain by another integer of the domain we will obtain as a result another integer of the domain, mod 13, is not so obvious. If z and y are any two integers of the domain our problem is to find another integer, x, of the set such that $xy \equiv z$, mod 13. If we assign to x all of the different values of the numbers of the set and multiply y by these different values of x (since multiplication is possible and unique) we shall obtain all of the numbers of the set once and only once. Since z is by hypothesis a number of the set, it is obtained when y is multiplied by some one of these particular values

---

* It might be interesting to note that this congruence holds with respect to a composite modulus, for example modulus 10. Suppose $x = 5$, $y = 4$, $y_1 = 2$, then we would have

$$x(y-y_1) \equiv 5(4-2) \equiv 0, \text{ mod } 10.$$

of x. We see therefore that z divided by x equals y, mod 13. Moreover this operation is in general unique, for if

$$z/x \equiv y, \text{mod } 13,$$

and also $$z/x_1 \equiv y, \text{ mod } 13, \text{ where } x_1 \neq x,$$

it would follow that $y(x-x_1) \equiv 0$, mod 13. For the same reasons which we stated in the proof of the uniqueness of multiplication this congruence will not hold unless $x_1 = x$.

We see therefore that division (excluding division by 0) in this set of numbers not only gives a number in the set, but also that this operation is in general unique.

Relation between the Roots of $X^{12} = 1$ and the Numbers of this Domain(0 excluded)

It is an interesting fact that if we take the twelve roots of the algebraic equation

$$X^{12} = 1,$$

we are able to establish a one to one correspondence as regards multiplication with the roots of this equation and the twelve numbers of this domain (0 excluded).

The twelve roots of

$$X^{12} = 1$$

are

$$\begin{aligned}
r_1 &= \cos 30^\circ + i \sin 30^\circ, \\
r_2 &= \cos 60^\circ + i \sin 60^\circ, \\
r_3 &= \cos 90^\circ + i \sin 90^\circ, \\
r_4 &= \cos 120^\circ + i \sin 120^\circ, \\
r_5 &= \cos 150^\circ + i \sin 150^\circ, \\
r_6 &= \cos 180^\circ + i \sin 180^\circ, \\
r_7 &= \cos 210^\circ + i \sin 210^\circ, \\
r_8 &= \cos 240^\circ + i \sin 240^\circ, \\
r_9 &= \cos 270^\circ + i \sin 270^\circ, \\
r_{10} &= \cos 300^\circ + i \sin 300^\circ, \\
r_{11} &= \cos 330^\circ + i \sin 330^\circ, \\
\text{and } r_{12} &= \cos 360^\circ + i \sin 360^\circ.
\end{aligned}$$

r_1 appertains*to exponent 12,
r_2 appertains to exponent 6,
r_3 appertains to exponent 4,
r_4 appertains to exponent 3,
r_5 appertains to exponent 12,
r_6 appertains to exponent 2,
r_7 appertains to exponent 12,
r_8 appertains to exponent 3,
r_9 appertains to exponent 4,
r_{10} appertains to exponent 6,
r_{11} appertains to exponent 12,
r_{12} appertains to exponent 1,

mod 13

1 appertains to exponent 1,
2 appertains to exponent 12,
3 appertains to exponent 3,
4 appertains to exponent 6,
5 appertains to exponent 4,
6 appertains to exponent 12,
7 appertains to exponent 12,
8 appertains to exponent 4,
9 appertains to exponent 3,
10 appertains to exponent 6,
11 appertains to exponent 12,
12 appertains to exponent 2,

mod 13

We see then that

$r_1 \sim 2$,** $r_7 \sim 11$,
$r_2 \sim 4$, $r_8 \sim 9$,
$r_3 \sim 8$, $r_9 \sim 5$,
$r_4 \sim 3$, $r_{10} \sim 10$,
$r_5 \sim 6$, $r_{11} \sim 7$,
$r_6 \sim 12$, $r_{12} \sim 1$.

This one to one correspondence as regards multiplication is possible because every prime number has primitive roots and every equation of the form

$$X^n - 1 = 0$$

has a primitive root, i,e., there is always one root whose powers give all the other roots.

The above is not the only manner in which the correspondence could have been established, for it is obvious that we could have

---

* When we say that a root or a number appertains to a certain exponent with respect to a given modulus, we mean that that number or root must be raised to the power indicated by that exponent in order that it be congruent to 1 with respect to the given modulus.

** The symbol $\sim$ denotes corresponds to.

associated the root, r_1, with the numbers, 6, 7, or 11, as well as with the number 2. But after this selection had been made the correspondence between the roots of the equation $X^{12} = 1$ and the numbers of the domain would have been uniquely determined.

A one to one correspondence with respect to the other fundamental operations is not possible because the roots of this equation do no constitute a domain.

Domain with respect to the Double Modulus, $(x^2-x-1, 3)$

The numbers of this domain may be so selected that they are

$$0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2.$$

The fact that addition, subtraction, multiplication and division (division by 0 excluded) in this set of numbers always give a number in the set with respect to mod$(x^2-x-1, 3)$ is established in exactly the same manner as in the domain with respect to the prime modulus 13. Similarly these operations are in general unique.

By the same method of reasoning as employed in the domain with respect to mod 13 we are able to establish a one to one correspondence with respect to multiplication between the roots of the equation

$$X^8 = 1$$

and the eight numbers of this domain (0 excluded).

The eight roots of

$$X^8 = 1$$

are

$$\begin{aligned} r_1 &= \cos 45^\circ + i \sin 45^\circ, \\ r_2 &= \cos 90^\circ + i \sin 90^\circ, \\ r_3 &= \cos 135^\circ + i \sin 135^\circ, \\ r_4 &= \cos 180^\circ + i \sin 180^\circ, \\ r_5 &= \cos 225^\circ + i \sin 225^\circ, \\ r_6 &= \cos 270^\circ + i \sin 270^\circ, \\ r_7 &= \cos 315^\circ + i \sin 315^\circ, \\ \text{and} \quad r_8 &= \cos 360^\circ + i \sin 360^\circ. \end{aligned}$$

r_1 appertains to exponent 8,
r_2 appertains to exponent 4,
r_3 appertains to exponent 8,
r_4 appertains to exponent 2,
r_5 appertains to exponent 8,
r_6 appertains to exponent 4,
r_7 appertains to exponent 8,
r_8 appertains to exponent 1,

mod $(x^2-x-1, 3)$

1 appertains to exponent 1,
2 appertains to exponent 2,
x appertains to exponent 8,
x+1 appertains to exponent 4,
x+2 appertains to exponent 8,
2x appertains to exponent 8,
2x+1 appertains to exponent 8,
2x+2 appertains to exponent 4.

mod $(x^2-x-1, 3)$

We therefore see that

$r_1 \sim x$, $r_5 \sim 2x$,
$r_2 \sim x+1$, $r_6 \sim 2x+2$,
$r_3 \sim 2x+1$, $r_7 \sim x+2$,
$r_4 \sim 2$, $r_8 \sim 1$.

This correspondence is possible for the same reason as stated in the domain with respect to mod 13. It is obvious that we could have also established this correspondence by associating r_1 with either $x+2$, $2x$, or $2x+1$. But after this selection had been made the correspondence would have been uniquely determined.

Domain with respect to the Double Modulus, $(x^2+x+1, 5)$

The numbers of this domain may be so chosen that they are 0, 1, 2, 3, 4, x, x+1, x+2, x+3, x+4, 2x, 2x+1, 2x+2, 2x+3, 2x+4, 3x, 3x+1, 3x+2, 3x+3, 3x+4, 4x, 4x+1, 4x+2, 4x+3, 4x+4.

In the same manner as in the domain with respect to mod 13 we are able to show that this set of numbers satisfies our definition of a domain of rationality and in general that these operations are unique with respect to mod $(x^2+x+1, 5)$.

Proceeding in a similar manner as in the two preceding domains

we are able to establish a one to one correspondence between the twenty-four numbers of this domain (0 excluded) and the roots of the algebraic equation

$$X^{24} = 1.$$

The roots of this equation are

$$\begin{aligned}
r_1 &= \cos 15^\circ + i \sin 15^\circ, \\
r_2 &= \cos 30^\circ + i \sin 30^\circ, \\
r_3 &= \cos 45^\circ + i \sin 45^\circ, \\
r_4 &= \cos 60^\circ + i \sin 60^\circ, \\
r_5 &= \cos 75^\circ + i \sin 75^\circ, \\
r_6 &= \cos 90^\circ + i \sin 90^\circ, \\
r_7 &= \cos 105^\circ + i \sin 105^\circ, \\
r_8 &= \cos 120^\circ + i \sin 120^\circ, \\
r_9 &= \cos 135^\circ + i \sin 135^\circ, \\
r_{10} &= \cos 150^\circ + i \sin 150^\circ, \\
r_{11} &= \cos 165^\circ + i \sin 165^\circ, \\
r_{12} &= \cos 180^\circ + i \sin 180^\circ, \\
r_{13} &= \cos 195^\circ + i \sin 195^\circ, \\
r_{14} &= \cos 210^\circ + i \sin 210^\circ, \\
r_{15} &= \cos 225^\circ + i \sin 225^\circ, \\
r_{16} &= \cos 240^\circ + i \sin 240^\circ, \\
r_{17} &= \cos 255^\circ + i \sin 255^\circ, \\
r_{18} &= \cos 270^\circ + i \sin 270^\circ, \\
r_{19} &= \cos 285^\circ + i \sin 285^\circ, \\
r_{20} &= \cos 300^\circ + i \sin 300^\circ, \\
r_{21} &= \cos 315^\circ + i \sin 315^\circ, \\
r_{22} &= \cos 330^\circ + i \sin 330^\circ, \\
r_{23} &= \cos 345^\circ + i \sin 345^\circ, \\
r_{24} &= \cos 360^\circ + i \sin 360^\circ.
\end{aligned}$$

r_1 appertains to exponent 24,
r_2 appertains to exponent 12,
r_3 appertains to exponent 8,
r_4 appertains to exponent 6,
r_5 appertains to exponent 24,
r_6 appertains to exponent 4,
r_7 appertains to exponent 24,
r_8 appertains to exponent 3,
r_9 appertains to exponent 8,
r_{10} appertains to exponent 12,
r_{11} appertains to exponent 24,
r_{12} appertains to exponent 2, $\mod(x^2+x+1, 5)$
r_{13} appertains to exponent 24,
r_{14} appertains to exponent 12,
r_{15} appertains to exponent 3,
r_{16} appertains to exponent 3,
r_{17} appertains to exponent 24,
r_{18} appertains to exponent 4,
r_{19} appertains to exponent 24,
r_{20} appertains to exponent 6,

r_{21} appertains to exponent 8,
r_{22} appertains to exponent 12,
r_{23} appertains to exponent 24,
r_{24} appertains to exponent 1.

1 appertains to exponent 1,
2 appertains to exponent 4,
3 appertains to exponent 4,
4 appertains to exponent 2,
x appertains to exponent 3,
x+1 appertains to exponent 6,
x+2 appertains to exponent 24,
x+3 appertains to exponent 8,
x+4 appertains to exponent 24,
2x appertains to exponent 12,
2x+1 appertains to exponent 8,
2x+2 appertains to exponent 12,
2x+3 appertains to exponent 24,
2x+4 appertains to exponent 24,
3x appertains to exponent 12,
3x+1 appertains to exponent 24,
3x+2 appertains to exponent 24,
3x+3 appertains to exponent 12,
3x+4 appertains to exponent 8,
4x appertains to exponent 6,
4x+1 appertains to exponent 24,
4x+2 appertains to exponent 8,
4x+3 appertains to exponent 24,
4x+4 appertains to exponent 3.

$\mod(x^2+x+1, 5)$

We see therefore that

$r_1 \sim x+2$,
$r_2 \sim 3x+3$,
$r_3 \sim x+3$,
$r_4 \sim 4x$,
$r_5 \sim 4x+1$,
$r_6 \sim 3$,
$r_7 \sim 3x+1$,
$r_8 \sim 4x+4$,
$r_9 \sim 3x+4$,
$r_{10} \sim 2x$
$r_{11} \sim 2x+3$,
$r_{12} \sim 4$,
$r_{13} \sim 4x+3$,
$r_{14} \sim 2x+2$,
$r_{15} \sim 4x+2$,
$r_{16} \sim x$,
$r_{17} \sim x+4$,
$r_{18} \sim 2$,
$r_{19} \sim 2x+4$,
$r_{20} \sim x+1$,
$r_{21} \sim 2x+1$,
$r_{22} \sim 3x$,
$r_{23} \sim 3x+2$,
$r_{24} \sim 1$.

It is clearly evident that we could have established this correspondence in other ways, for we could have associated r_7 with either one of the numbers of the domain which appertained to exponent 24. But after this selection had been made the correspondence would have been uniquely determined.

Equations irreducible with respect to this domain

Having given a domain K, the definition of irreducibility would be stated in the following manner: an equation, the coefficients of which appertain to the domain K is said to be irreducible when it can not be reduced to the product of two rational integral functions in x, with rational coefficients in K, and of degree different from zero. In our domain an equation is irreducible when it can not be expressed as the product of two numbers of the domain, mod$(x^2+x+1, 5)$.

Excluding the case where the coefficient of x is zero, for such a situation would leave us an equation of the first degree, it is easily seen that there are one hundred quadratic expressions with respect to mod$(x^2+x+1, 5)$. Of these one hundred expressions those which are irreducible are marked with an *; those which are reducible have been expressed as the product of two of the numbers of the domain, mod$(x^2+x+1, 5)$.

x^2+x+1^*
$2x^2+x+1^*$
$3x^2+x+1 \equiv (3x+2)(x+3)$
$4x^2+x+1 \equiv (x+2)(4x+3)$
$x^2+2x+1 \equiv (x+1)(x+1)$
$2x^2+2x+1 \equiv (x+2)(2x+3)$
$3x^2+2x+1^*$
$4x^2+2x+1^*$
$x^2+3x+1 \equiv (4x+1)(4x+1)$
$2x^2+3x+1 \equiv (2x+1)(x+1)$
$3x^2+3x+1^*$
$4x^2+3x+1^*$
x^2+4x+1^*
$2x^2+4x+1^*$
$3x^2+4x+1 \equiv (3x+1)(x+1)$
$4x^2+4x+1 \equiv (2x+1)(2x+1)$
x^2+x+2^*
$2x^2+x+2 \equiv (3x+2)(4x+1)$
$3x^2+x+2^*$
$4x^2+x+2 \equiv (2x+1)(2x+2)$
$x^2+2x+2 \equiv (x+3)(x+4)$
$2x^2+2x+2^*$
$3x^2+2x+2 \equiv (2x+4)(4x+3)$
$4x^2+2x+2^*$

$x^2+3x+2 \equiv (4x+3)(4x+4)$
$2x^2+3x+2^*$
$3x^2+3x+2 \equiv (3x+4)(x+3)$
$4x^2+3x+2^*$
x^2+4x+2^*
$2x^2+4x+2 \equiv (2x+2)(x+1)$
$3x^2+4x+2^*$
$4x^2+4x+2 \equiv (4x+1)(x+2)$
$x^2+x+3 \equiv (x+2)(x+4)$
$2x^2+x+3^*$
$3x^2+x+3 \equiv (3x+3)(x+1)$
$4x^2+x+3^*$
x^2+2x+3^*
$2x^2+2x+3 \equiv (2x+1)(x+3)$
$3x^2+2x+3^*$
$4x^2+2x+3 \equiv (4x+3)(x+1)$
x^2+3x+3^*
$2x^2+3x+3 \equiv (2x+4)(x+2)$
$3x^2+3x+3^*$
$4x^2+3x+3 \equiv (4x+1)(x+3)$
$x^2+4x+3 \equiv (x+1)(x+3)$
$2x^2+4x+3^*$
$3x^2+4x+3 \equiv (3x+2)(x+4)$
$4x^2+4x+3^*$

$x^2+x+4 \equiv (2x+1)(3x+4)$
$2x^2+x+4 \equiv (2x+4)(x+1)$
$3x^2+x+4$*
$4x^2+x+4$*
x^2+2x+4*
$2x^2+2x+4$*
$3x^2+2x+4 \equiv (3x+4)(x+1)$
$4x^2+2x+4 \equiv (4x+1)(x+4)$
x^2+3x+4*
$2x^2+3x+4$*
$3x^2+3x+4 \equiv (3x+2)(x+2)$
$4x^2+3x+4 \equiv (4x+4)(x+1)$
$x^2+4x+4 \equiv (x+2)(x+2)$
$2x^2+4x+4 \equiv (2x+3)(x+3)$
$3x^2+4x+4$*
$4x^2+4x+4$*

$x^2+x \equiv x(x+1)$
$2x^2+x \equiv x(2x+1)$
$3x^2+x \equiv x(3x+1)$
$4x^2+x \equiv x(4x+1)$
$x^2+2x \equiv x(x+2)$
$2x^2+2x \equiv 2x(x+1)$
$3x^2+2x \equiv x(3x+2)$
$4x^2+2x \equiv x(4x+2)$
$x^2+3x \equiv x(x+3)$
$2x^2+3x \equiv x(2x+3)$
$3x^2+3x \equiv x(3x+3)$
$4x^2+3x \equiv x(4x+3)$
$x^2+4x \equiv x(x+4)$
$2x^2+4x \equiv x(2x+4)$
$3x^2+4x \equiv x(3x+4)$
$4x^2+4x \equiv x(4x+4)$
$x^2+1 \equiv (x+2)(x+3)$
$2x^2+1$*
$3x^2+1$*
$4x^2+1 \equiv (x+1)(4x+1)$
x^2+2*
$2x^2+2 \equiv (x+2)(2x+1)$
$3x^2+2 \equiv (x+1)(3x+2)$
$4x^2+2$*
x^2+3*
$2x^2+3 \equiv (x+1)(2x+3)$
$3x^2+3 \equiv (x+2)(3x+4)$
$4x^2+3$*
$x^2+4 \equiv (x+1)(x+4)$
$2x^2+4$*
$3x^2+4$*
$4x^2+4 \equiv (x+2)(4x+2)$

$x^2 \equiv x \cdot x$
$2x^2 \equiv x \cdot 2x$
$3x^2 \equiv x \cdot 3x$
$4x^2 \equiv x \cdot 4x$

If we take any one of these irreducible quadratic expressions along with 5 as a double modulus, we are able to set up a finite domain which will contain the same set of twenty-five numbers which are in the domain with respect to the double modulus, $(x^2+x+1, 5)$. In this new domain will be found the same number of numbers which appertain to exponents 1, 2, 3, 4, 6, 8, 12 and 24.

With respect to mod $(x^2+x+2, 5)$

1 appertains to exponent 1,
2 appertains to exponent 4,
3 appertains to exponent 4,
4 appertains to exponent 2,
x appertains to exponent 24,
x+1 appertains to exponent 24,
x+2 appertains to exponent 12,
x+3 appertains to exponent 8,
x+4 appertains to exponent 12,
2x appertains to exponent 24,
2x+1 appertains to exponent 8,
2x+2 appertains to exponent 24,
2x+3 appertains to exponent 3,
2x+4 appertains to exponent 6,

$3x$ appertains to exponent 24,
$3x+1$ appertains to exponent 3,
$3x+2$ appertains to exponent 6,
$3x+3$ appertains to exponent 24,
$3x+4$ appertains to exponent 8,
$4x$ appertains to exponent 24,
$4x+1$ appertains to exponent 12,
$4x+2$ appertains to exponent 8,
$4x+3$ appertains to exponent 12,
$4x+4$ appertains to exponent 24.

Either one of the numbers which appertains to exponent 24, mod $(x^2+x+2, 5)$ when raised to successive powers will give all the numbers of the set; for example

$(x) \equiv x,$
$(x)^2 \equiv x^2 \equiv 4x+3,$
$(x)^3 \equiv 4x^2+3x \equiv 4x+2,$
$(x)^4 \equiv 4x^2+2x \equiv 3x+2,$
$(x)^5 \equiv 3x^2+2x \equiv 4x+4,$
$(x)^6 \equiv 4x^2+4x \equiv 2,$
$(x)^7 \equiv 2x$
$(x)^8 \equiv 2x^2 \equiv 3x+1,$
$(x)^9 \equiv 3x^2+x \equiv 3x+4,$
$(x)^{10} \equiv 3x^2+4x \equiv x+4,$
$(x)^{11} \equiv x^2+4x \equiv 3x+3,$
$(x)^{12} \equiv 3x^2+3x \equiv 4,$
$(x)^{13} \equiv 4x,$
$(x)^{14} \equiv 4x^2 \equiv x+2,$
$(x)^{15} \equiv x^2+2x \equiv x+3,$
$(x)^{16} \equiv x^2+3x \equiv 2x+3,$
$(x)^{17} \equiv 2x^2+3x \equiv x+1,$
$(x)^{18} \equiv x^2+x \equiv 3,$
$(x)^{19} \equiv 3x$
$(x)^{20} \equiv 3x^2 \equiv 2x+4,$
$(x)^{21} \equiv 2x^2+4x \equiv 2x+1,$
$(x)^{22} \equiv 2x^2+x \equiv 4x+1,$
$(x)^{23} \equiv 4x^2+x \equiv 2x+2,$
$(x)^{24} \equiv 2x^2+2x \equiv 1.$

Bibliography

L. W. Reid: The Elements of the Theory of Algebraic Numbers.

F. Cajori: Theory of Equations.

L. E. Dickson: Elementary Theory of Equations.

G. B. Matthews: Theory of Numbers, Part I.

E. Cahen: Eléments de la Théorie des Nombres.

D. Hilbert: Théorie des Corps de Nombres Algébriques.

J. Sommer: Introduction à la Théorie des Nombres Algébriques.

H. Weber: Traité d'Algèbre Supérieure.

Ed. Lucas: Théorie des Nombres.

Burnside and Panton: Theory of Equations.

Encyclopédie des Sciences Mathématiques, Tome I, Vol. 2.

Journal für die Mathematik, Vol. 92.